Calhoun: The NPS Institutional Archive

DSpace Repository

Theses and Dissertations | 1. Thesis and Dissertation Collection, all items

2007-09

Modern advances to the Modular Fly-Away Kit (MFLAK) to support maritime interdiction operations

Cross, Eric C.

Monterey California. Naval Postgraduate School

http://hdl.handle.net/10945/3321

Downloaded from NPS Archive: Calhoun

http://www.nps.edu/library

Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

MODERN ADVANCES TO THE MODULAR FLY-AWAY KIT (MFLAK) TO SUPPORT MARITIME INTERDICTION OPERATIONS

by

Eric C. Cross

September 2007

Thesis Advisor:	James Ehlert
Co-Advisor:	Gurminder Singh

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 2007	Master's Thesis

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Modern Advances to the Modular Fly-Away Kit (MFLAK) to Support Maritime Interdiction Operations	
6. AUTHOR(S) Eric C. Cross	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES: The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT	12b. DISTRIBUTION CODE
Approved for public release; distribution is unlimited	

13. ABSTRACT (maximum 200 words)

This thesis will test the performance of an end-to-end network solution designed to augment Maritime Interdiction Operations that support boarding parties and their near real time communications with supporting agencies. The 802.16 point-to-point and point-to-multipoint Orthogonal Frequency Divisional Multiplexing (OFDM) shall be upgraded to reflect modern advances in 802.16. Additionally, there will be several enhancements to the peripherals associated with end user innovations and they will include: upgraded biometric devices, innovative camera solutions for near real time viewing, laptop support, airborne operations and communications devices for augmenting radio systems. Specifically, this thesis evaluates the enhanced effectiveness of implementing 802.16 networking equipment into the communications suite of several sea platforms. The test portions of this thesis will include laboratory specifications, bench test analysis and field experimentation done in partnership with the Cooperative Operations and Applied Science & Technology Studies (COASTS).

COASTS is a combined Indonesia-Malaysia-Singapore-Thailand-U.S. R&D effort to investigate commercial-off-the-shelf (COTS) Command and Control, Communications Computers and Intelligence, Surveillance and Reconnaissance (C4ISR) technologies to provide real-time situational awareness (SA) for multi-national, tactical and remote decision makers in a cooperative environment. The capstone field experiment is conducted annually in May and June. COASTS-07 is the third iteration in the series and built on the successes and lessons learned from the 2005 and 2006 field experiments. In 2007, COASTS also employed some technologies into two major multi-national Pacific Fleet exercises, specifically US Pacific Fleet's exercise TALISMAN SABER 2007 with COMSEVENTHFLT in Australia during June 2007 and COMLOG WESTPAC's Southeast Asia Cooperation Against Terrorism (SEACAT) 2007 exercise in Singapore during August 2007.

14. SUBJECT TERMS	15. NUMBER OF PAGES
802.11b, 802.11g, Wi-Fi, SecNet-11, 802.16, WIMAX, MIMO, OFDM, COTS, Integrated Common Operational Picture, Maritime Interdiction Operations, WLAN, Bridging, Tactical Internet, Biometrics, Boarding, Backhaul, COASTS, FLAK, MFLAK	135
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

MODERN ADVANCES TO THE MODULAR FLY-AWAY KIT (MFLAK) TO SUPPORT MARITIME INTERDICTION OPERATIONS

Eric C. Cross
Captain, United States Marine Corps
B.S. in Business Administration, University of Arizona, 2001

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2007

Author: Eric C. Cross

Approved by: Mr. James Ehlert
Thesis Advisor

Dr. Gurminder Singh
Co-Advisor

Dr. Dan C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis will test the performance of an end-to-end network solution designed to augment Maritime Interdiction Operations that support boarding parties and their near real time communications with supporting agencies. The 802.16 point-to-point and point-to-multipoint Orthogonal Frequency Divisional Multiplexing (OFDM) shall be upgraded to reflect modern advances in IEEE 802.16. Additionally, there will be several enhancements to the peripherals associated with end user innovations and they will include: upgraded biometric devices, innovative camera solutions for near real time viewing, laptop support, airborne operations and communications devices for augmenting radio systems. Specifically, this thesis evaluates the enhanced effectiveness of implementing 802.16 networking equipment into the communications suite of several sea platforms. The test portions of this thesis will include laboratory specifications, bench test analysis and field experimentation done in partnership with the Cooperative Operations and Applied Science & Technology Studies (COASTS).

COASTS is a combined Indonesia-Malaysia-Singapore-Thailand-U.S. R&D effort to investigate commercial-off-the-shelf (COTS) Command and Control, Communications Computers and Intelligence, Surveillance and Reconnaissance (C4ISR) technologies to provide real-time situational awareness (SA) for multi-national, tactical and remote decision makers in a cooperative environment. The capstone field experiment is conducted annually in May and June. COASTS-07 is the third iteration in the series and built on the successes and lessons learned from the 2005 and 2006 field experiments. In 2007, COASTS also employed some technologies into two major multi-national Pacific Fleet exercises, specifically US Pacific Fleet's exercise TALISMAN SABER 2007 with COMSEVENTHFLT in Australia during June 2007 and COMLOG WESTPAC's Southeast Asia Cooperation Against Terrorism (SEACAT) 2007 exercise in Singapore during August 2007.

.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
- **A. BACKGROUND....1**
- **B. OBJECTIVES....7**
- **C. RESEARCH QUESTIONS....8**
- **D. SCOPE....9**
- **E. METHODOLOGY....9**
- **F. ORGANIZATION OF THESIS....10**

II. MARITIME INTERDICTION OPERATIONS....13
- **A. NETWORK CENTRIC WARFARE....13**
- **B. NATIONAL STRATEGY FOR MARITIME SECURITY....17**
- **C. DEPARTMENT OF HOMELAND SECURITY....18**
- **D. COASTS....20**

III. COMPONENT SELECTION FOR MFLAK II....23
- **A. MISSION....23**
- **B. TOPOLOGY....24**
  - **1. COASTS 2006 Background....24**
  - **2. COASTS 2007 Background....25**
- **C. MOBILE COMPUTING....27**
  - **1. Routing Equipment....29**
    - ***a. ComCase T....29***
    - ***b. ComCase G....30***
    - ***c. ComCase E....30***
    - ***d. ComCase H....31***
    - ***e. Grizzly....33***
  - **2. IEEE 802.11 AND 802.16 PRODUCTS FOR CONNECTION AND BACKHAUL....34**
    - ***a. Redline AN-80i IEEE 802.16 Radio Transmitter....35***
    - ***b. Motorola Spectra PTP 600 IEEE 802.16 MIMO Radio Transmitter....36***
    - ***c. Fortress ES-520 IEEE 802.11 Radio Transmitter....37***
    - ***d. Cisco 2.4GHz Wireless Mobile Interface Card (WMIC) IEEE 802.11 Radio Transmitter....38***
  - **3. NETWORK SECURITY....38**
    - ***a. Biometric Device - SutiSoft Secured BioNet (SBN) Fingerprint Scanner....39***
    - ***b. Biometric Device – DynaSig Bio Pen....40***
    - ***c. Biometric Device – Identix RDT4....41***
  - **4. PORTABLE COMPUTING DEVICES....42**
    - ***a. OQO Wearable Computing Device....42***
  - **5. INTERNET PROTOCOL (IP) VIDEO EQUIPMENT....44**
    - ***a. XVD....44***

b. AXIS-213 Cameras 45
c. Integrated Common Operational Picture (iCOP) 46
D. SUMMARY 47

IV. SELECTION OF METRICS AND EXPERIMENT DESIGN 49
A. SCOPE OF THE TEST 51
B. SELECTED METRICS 53
C. MEASURES OF EFFECTIVENESS AND PERFORMANCE 54
1. Test Equipment 55
2. Testing Equipment 55
D. TESTING 56
E. GENERAL OBSERVATIONS 60

V. MARITIME FLY AWAY KIT GENERATION II 63
A. COMPOSITION 63
1. Garrison Components 63
2. Mobile Components 63
3. Mission Enhanced Components 65
B. STANDARD OPERATING PROCEDURES (SOP) 67
1. Preparation of Equipment 67
2. Testing of Equipment 68
3. Operation of Equipment 68
C. SUMMARY 69

VI. CONCLUSION AND RECOMMENDATIONS 71
A. CONCLUSION 71
1. Key Findings 72
a. Ruggedized Equipment that is Not Rack Mountable 72
b. Mobile Networks Exist to Support Operations 72
c. Technology is Not the Only Answer 72
d. Deployment Scenarios Must be Realistic 73
B. CONCLUDING REMARKS 73
1. Future Research 73
a. PC/104 Form Factor 73
b. Software Development 74
c. Power Consumption and Distribution 74
2. SUMMARY 75

APPENDIX A –ROUTER CONFIGURATIONS 77

APPENDIX B – FIELD TRAINING EXERCISE DIAGRAMS 87

APPENDIX C – FIELD EXERCISES 91

APPENDIX D – COTS TECHNICAL SPECIFICATIONS 99

APPENDIX E - THAILAND FIELD TEST EXERCISE 103

LIST OF REFERENCES 111

INITIAL DISTRIBUTION LIST 113

LIST OF FIGURES

Figure 1. VBSS operation in the Indian Ocean with Joint forces. (From Associated Press)....4
Figure 2. USCG Operations in Mona Passage.(From Associated Press)....5
Figure 3. COASTS Multi-Agency Partnership Chart 6
Figure 4. C4ISR Architecture Framework. (From Joint Vision 2010) 8
Figure 5. Role of Experimentation in the Coevolution of MCPs. (From Footnote 16) ..14
Figure 6. Virtual Collaboration—Moving Information, Not People (From Footnote 21) 17
Figure 7. Mobile nodes roaming across multiple networks. (From www.cisco.com) 24
Figure 8. COASTS Topology 2006....25
Figure 9. COASTS 2007 Topology....27
Figure 10. ComCase T from Technical Brochure. (From www.westerndata.com) 30
Figure 11. ComCase E from technical brochure. (From www.westerndata.com) 31
Figure 12. COMCASE H ROUTER from Technical Specifications. (From www.westerndata.com)....32
Figure 13. Grizzly from Technical Brochure. (From www.westerndata.com) 34
Figure 14. Redline AN-80i - IEEE 802.16 Radio Transmitter Setup. (From AN-80i User Manual) 36
Figure 15. Motorola PTP 600 Tech Specifications. (From Motorola PTP600 User Manual)....37
Figure 16. Cisco 3200 Wireless and Mobile Router with 2.4 GHz IEEE 802.11b/g WMIC. (From www.westerndata.com) 38
Figure 17. Secured BioNet (SBN - SutiSoft) Server & Finger Print Device. (From SutiSoft User Manual) 40
Figure 18. Bio Pen Enterprise Edition. (From DynaSig Bio-Pen User Manual) 41
Figure 19. Historical perspective from laptop/cell phone to UMPC/Smartphone. (From www.oqo.com)....43
Figure 20. OQO Model 01 (Top) and Model 02 (Bottom). 43
Figure 21. XVD CamCast for Multicasting operations....45
Figure 22. Axis 213 IP Camera with PTZ. (From www.axis.com) 46
Figure 23. Integrated Common Operational Picture (iCOP) Display. (From COASTS)..47
Figure 24. Maritime Fly Away Kit – Gen II (MFLAKII) as configured for SEACAT 2007....48
Figure 25. Fort Hunter-Liggett Army Base in California. (From GoogleEarth)....50
Figure 26. Mae Ngat Dam in Thailand. (From GoogleEarth)....51
Figure 27. High Level Topology for Camp Roberts, California. (From GoogleEarth) 52
Figure 28. Network Diagram for Field Exercise II, Fort Hunter Liggett, California....52
Figure 29. Response Time for Test 1, 2 and 3 on Back Haul Radio Transmitters....57
Figure 30. Throughput for Test 1, 2 and 3 on Back Haul Radio Transmitters....58
Figure 31. Video Streaming for Test 1, 2 and 3 on Back Haul Radio Transmitters 59
Figure 32. MFLAK Grizzly mounted on CDR Schmidt's Cessna....64
Figure 33. Grizzly faceplates configured with IVS at UAV Site....65

Figure 34. Wrist mounted mapping device with USB connection. 66
Figure 35. Boarding Party components for two personnel. 66

LIST OF ACRONYMS AND ABBREVIATIONS

AAR	After Action Report
AES	Advanced Encryption Standard
AFRL	Air Force Research Laboratory
AOR	Area of Responsibility
AT/FP	Antiterrorism/Force Protection
ATCD	Advanced Technology Concept Demonstration
C2	Command and Control
C2W	Command and Control Warfare
C4	Command, Control, Communications, and Computer
C4I	Command and Control, Communications, Computers and Intelligence
C4ISR	Command and Control, Communications Computers and Intelligence, Surveillance and Reconnaissance
CA	Civil Affairs
CBC	Cipher Block Chaining
CCMP	Counter-Mode CBC MAC Protocol
CDC	Concept Development Conference
CDR	Commander
CFACC	Combined Force Air Component Commander
CINC	Commander in Chief
CJTF	Combined Joint Task Force
CMA	Cooperative Maritime Agreement
CNO	Chief of Naval Operations
COASTS	Cooperative Operations and Applied Science & Technology Studies
CONOPS	Concept of Operations
COTS	Commercial-off-the-Shelf
CPX	Command Post Exercise
CT	Combating Terrorism
DA	Direct Action
DC&A	Data Collection and Analysis
DCAP	Data Collection and Analysis Plan

DEA	Drug Enforcement Agency
DHS	Department of Homeland Security
DoD	Department of Defense
DON	Department of the Navy
DRDO	Defense Research Development Organization
EMIO	Extended Maritime Interdiction Operations
FID	Foreign Internal Defense
FLAK	Fly-Away Kit
FPC	Final Planning Conference
FTX	Field Training Exercise
FY07	Fiscal Year 2007
GHz	Gigahertz
GNOC	Global Network Operations Center
GPS	Global Positioning System
GUI	Graphical User Interface
GWOT	Global War on Terrorism
IEEE	Institute of Electrical and Electronic Engineers
IIFC	Interagency Intelligence Fusion Center
IO	Information Operations
IPC	Initial Planning Conference
ISR	Intelligence, Surveillance and Reconnaissance
JIATF	Joint Interagency Task Force
JIOWC	Joint Information Operations Warfare Command
JTF	Joint Task Force
JUSMAGTHAI	Joint US Military Advisory Group, Thailand
LAN	Local Area Network
LIO	Leadership Interdiction Operation
LLNL	Lawrence Livermore National Laboratory
LNO	Liaison Officer
MAC	Message Authentication Code
MALSINDO	Malaysia, Indonesia and Singapore

Mbps	Megabits per Second
MCP	Mission Capability Package
MCSC	Marine Corps Systems Command
MDA	Maritime Domain Awareness
MDP-RG	Maritime Domain Protection Research Group
METOC	Meteorological and Oceanographic
MIO	Maritime Interdiction Operations
MMEA	Malaysian Maritime Enforcement Agency
MNF	Multinational Force
MOE	Measure of Effectiveness
MOP	Measure of Performance
MPC	Mid Planning Conference
MUA	Military Utility Analysis
mW	milliWatt
NCW	Network Centric Warfare
NEMA	National Electrical Manufacturers Association
NGO	Non-Governmental Organization
NOC	Network Operations Center
NPS	Naval Postgraduate School
NPSSOCFEP	Naval Postgraduate School Special Operations Command Field Experimentation Program
NSTM	Naval Ship Technical Manual
NSW	Naval Special Warfare
OCONUS	Outside Continental United States
ODC	Office of Defense Cooperation
OFDM	Orthogonal Frequency-Division Multiplexing
OM	Operational Manager
ONR	Office of Naval Research
OPORD	Operations Order
OSD	Office of the Secretary of Defense
PEO	Program Executive Office
PM	Program Manager

POC	Point of Contact
PSYOPS	Psychological Operations
R&D	Research and Development
RF	Radio Frequency
RHIB	Rigid Hull Inflatable Boat
RMA	Reliability, Maintainability and Availability
RMSI	Regional Maritime Security Initiative
RTAF	Royal Thai Air Force
RTARF	Royal Thai Armed Forces
RTN	Royal Thai Navy
S&T	Science & Technology
SA	Situational Awareness
SBU	Small Boat Unit
SEACAT	Southeast Asia Cooperation Against Terrorism
SNMP	Simple Network Management Protocol
SOCOM	Southern Operations Command
SOF	Special Operations Force
SOP	Standard Operating Procedure
SSID	Service Set Identifier
TM	Technical Manager
TNT FE	Tactical Network Topology Field Experiment
TOC	Tactical Operations Center
TR	Tactical Reconnaissance
TTPs	Techniques, Tactics and Procedures
UAV	Unmanned Aerial Vehicle
UNODC	United Nations Office of Drugs & Crime
USAF	United States Air Force
USCG	United States Coast Guard
USMC	United States Marine Corps
USN	United States Navy
USPACOM	US Pacific Command
USSOCO	US Special Operations Command

VBSS	Visit Board, Search, and Seizure
VLAN	Virtual LAN
VOIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
Wi-Max	Broadband Wireless
WLAN	Wireless Local Area Network
WMD	Weapons of Mass Destruction
WPA	Wi-Fi Protected Access
WWAN	Wireless Wide Area Network

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First and foremost, I would like to thank my children, Allibeth and Jacob, for their understanding and patience during the last two years. Their smiles, alone, are enough to keep me going everyday. A special thanks to my dad who has always been there and supported me no matter what. And last, but not least, I would like to thank my loving wife, Renee, for her patience and support during this arduous process. She is the strength in my life, my marriage and my future and none of this would be possible without her friendship, love and support.

Additionally, I would like to personally thank Jim Ehlert for his guidance during this process. His expertise and real world experience (as well as a few Beer Changs) made this thesis relevant and worthy despite the number of hours and travel requirements necessary to complete it. Also, I would like to thank Dr. Gurminder Singh for his support, travel and guidance throughout this process and all of the COASTS students, vendors and staff that made the last two years a tremendous learning experience.

Lastly, I would like to thank Major Erdie, Marine Corps Systems Command, for funding this project, Clay Porter and Ryan Hale for sharing their networking expertise, as well as, Dr. Shoup for his continued support from the Maritime Interdiction Operations perspective.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

On June 6, 2007, the USS Mahan (DDG72) participated in a combined Maritime Interdiction Operations (MIO) with the Russian frigate, RFS Neustrashimy (RFS 712), as part of the Baltic Operations (BALTOPS) 2007. BALTOPS is the largest annual international training event organized in the Baltic Sea and includes in-port and at-sea serialized training events designed to build interoperability and better information-sharing practices with partnering nations. The two ships took part in MIO operations -- the inspection and possible diversion of suspect merchant vessels -- as one of the first events of the multiphase exercise. During the training event, small boats from Mahan with a boarding team from Neustrashimy practiced boarding procedures aboard the suspect cargo ship simulated by another player in the exercise, USNS LCPL Roy M. Wheat (T-AK 3016). The U.S.-led invitational exercise involved 25 ships, two submarines and several air assets over the course of the 11-day event. Participants included: United States, Denmark, Germany, Russia, the Netherlands, Lithuania, Latvia, France, Poland, Sweden and the United Kingdom with the combined goal of promoting mutual understanding, confidence, cooperation, and interoperability among forces and personnel of participating nations.[1] Ultimately, Maritime Domain Awareness (MDA) is about collecting and sharing large amounts of data[2] and information[3]. This data can be aggregated to enhance a Common Operational Picture (COP) that allows Global Network Operations Centers (GNOC) and Network Operations Centers (NOC) to disseminate information to key leaders while maintaining the integrity[4] and authenticity[5] of the data

[1] "Mahan Participates in .MIO Drillwith Russian FrigateDuring BALTOPS 2007." Navy News Stand, June 2007.

[2] Data: a collection of facts from which conclusions may be drawn; "statistical data."

[3] Information: the result of processing, manipulating and organizing data in a way that adds to the knowledge of the person receiving it.

[4] Integrity: a security service that ensures that modifications to data are detectable.

[5] Authenticity: the trustworthiness of data or an entity. The authenticity can be secured and verified using cryptographic methods.

being passed. By utilizing this data through a COP, it becomes actionable intelligence (e.g., a boarding officer processing real-time information and processing it quick enough to make decisions so that assailants are not released when they should have been detained) to be used by agencies and entities to enhance their MIOs, Terrorist Operations and Maritime Law enforcement operations. Information sharing is a necessity within MDA if our multi-national network is going to be effective in detection, identification and tracking of perceived threats. These threats pose serious security concerns through the importation of narcotics, pirated goods, Weapons of Mass Destruction (WMD) and services, such as human trafficking, arms trafficking and illegal immigration. Compounding the security concerns is the ability for crimes to propagate through international waters, thus making this a multi-national issue. Information sharing must not only exist in the U.S., but throughout the world in order to track and maintain proper communications channels that aide in the detection and capture of these criminal activities. Understanding and dealing with these threats opens a wide area of operations; it is relevant that our national partners design and provide a network that is capable of information sharing that will enhance MIOs in a global sense and maintain these engagements at distances that do not impact the daily lives of our citizens.

The National Strategy for Maritime Security aligns all government maritime security programs and initiatives into a comprehensive and cohesive national effort involving appropriate federal, state and local entities. It outlines eight supporting plans that target specific threats and challenges in the maritime environment.

- National Plan to Achieve Domain Awareness
- Global Maritime Intelligence Integration Plan
- Interim Maritime Operational Threat Response Plan
- International Outreach and Coordination Strategy
- Maritime Infrastructure Recovery Plan
- Maritime Transportation System Security Plan
- Maritime Commerce Security Plan
- Domestic Outreach Plan

The National Strategy addresses the need for global coverage and identifies the world's saltwater areas as a vital part (2/3's of the earth's surface) of that effort.

> Unprecedented advances in telecommunications and dramatic improvements in international commercial logistics have combined to

> increase both the range and effects of terrorist activities, providing the physical means to transcend even the most secure borders and to move rapidly across great distances. Adversaries that take advantage of such transnational capabilities have the potential to cause serious damage to global, political, and economic security. The maritime domain in particular presents not only a medium by which these threats can move, but offers a broad array of potential targets that fit the terrorists' operational objectives of achieving mass casualties and inflicting catastrophic economic harm.[6] [7]

In the 2007 Chief of Naval Operations Guidance (CNOG), Admiral Mullen focuses on the execution stage of a plan that includes "three main priorities: sustaining combat readiness; building a fleet for the future; and developing 21st Century leaders."[8] The CNOG addresses the Maritime Strategy in terms of combining a traditional Navy with an enhanced Navy capable of confronting and influencing the highly dynamic security environment of the 21st Century, which, includes our future leaders and the fleet of the future. The 1,000-ship Navy, now referred to as Global Maritime Force (GMF), covers a breadth of countries that have come together to join a multi-national naval effort that works to combine worldwide naval assets to address global problems. One of the most important notes in the CNOG is regional MDA and the implementation of small boats[9] into the GMF. Adding to this concept is the Global Fleet Station (GFS), which is a persistent sea base of operations focusing primarily on shaping operations and global maritime awareness. The GFS deployment is designed to analyze the GFS concept for the Navy and support U.S. Southern Command (SOUTHCOM) objectives for its area of responsibility by enhancing cooperative partnerships with regional maritime services and improving operational readiness for the participating partner nations.[10] With this joint

---

[6] Department of Homeland Security, National Security Strategy on Maritime Security, September 2005.

[7] The maritime domain is defined as all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances.

[8] Department of the Navy, Chief of Naval Operations Guidance 2007.

[9] Since 2001, the Navy began procurement of Commercial-Off-The-Shelf (COTS) small boats and craft that are used to support harbor patrol and security efforts, drug interdiction, search, air, and rescue (SAR), line handling duties, barrier tending, and escort duties.

[10] Global Fleet Station Pilot One Step Closer with Arrival of Swift.

venture, Admiral Stavridis, (CDRUSSOCOM) and the GFS program will focus on patrol craft operations that include inter-service communications in a riverine environment.

In supporting these plans, the Department of Homeland Security (DHS), has issued the Mona Passage Proof of Concept.[11] This program will support the National Strategy on Maritime Security through the extension of mobile biometric collections on maritime vessels. The United States Coast Guard (USCG) shall deploy a method of at-sea screening of various targets: smugglers, immigrants, drug traffickers and human traffickers. The information collected shall be downloaded to a *non-networked laptop* for future processing.

Figure 1. VBSS operation in the Indian Ocean with Joint forces.
(From Associated Press)

[11] Deparment of Homeland Security, Mona Passage Proof of Concept, November 2006.

Figure 2. USCG Operations in Mona Passage.(From Associated Press)

The early phases of this program lead to a problem shared by all components of the US military and multi-national agents; that is the problem with processing data in a real-time communications environment. The capability of transferring the processed information, so that it can be handled expeditiously, automatically and in real time, so that the boarding officers do not have to end the maritime engagement without a positive match scenario.

The NPS Cooperative Operations and Applied Science & Technology Studies (COASTS) international field experimentation program guides off of the National Strategy, the CNO's strategy and the USCG's strategy and employment. COASTS focuses on a combined Indonesia-Malaysia-Singapore-Thailand-U.S. R&D effort to investigate commercial-off-the-shelf (COTS) Command and Control, Communications Computers and Intelligence, Surveillance and Reconnaissance (C4ISR) technologies to provide real-time situational awareness (SA) for multi-national, tactical and remote decision makers in a cooperative environment.

Figure 3. COASTS Multi-Agency Partnership Chart.

In summary, the National Strategy for Maritime Security lays out a path that incorporates all federal, state and local agencies to share data in the maritime environment. The CNO has laid out a plan to support a GMF that is capable of handling the world's littorals. This combination allows for global partnership in extending security to our waterways while integrating national resources to support the Maritime Security environment. Subsequently, the Department of Homeland Security (DHS) has embarked on a program that will provide the tools and assets necessary to collect biometric data and personal data on all interdiction operations with respect to guarding America's borders. This collection of data is vital and serves multiple nations with the information database that keeps track of well known exploits and violations across global waterways. The logical conclusion and next step in this process is to take the collected biometric data and transport it to the proper agencies. By utilizing a near-real time platform that can use the multi-national agencies to scan, process and authenticate the data and give feedback to the boarding party officer so that they have information that is relevant to their search, timely for their interdiction and available during the boarding

operation embarked upon. Lastly, the COASTS program leverages their technology partners and provides real world field experimentation that addresses the needs and desires of the National components. It is through this venue, that solutions and demonstrations can be conducted, with component participation and feedback. This allows the COASTS program to strengthen and grow by addressing these high level needs and deploying technologies that, ultimately, support the war fighter at home and abroad.

B. OBJECTIVES

This research is used to capture environmental conditions of operating a mobile network[12] and adjusting to the needs of the war fighter while maintaining stationary and mobile communications platforms. This research expands network communications to water borne assets to support riverine and maritime operations, thus combining the efforts of mobile and garrison networks and providing a network platform capable of real time communications in an "at sea" environment.[13]

The ultimate goal is to provide similar network capabilities currently available in a garrison environment and extend them to the mobile operators. In a ground environment, the mobile operators normally conduct exercises through foot patrols and vehicle patrols. In a maritime environment, the small boat operator is the lowest echelon requiring mobile communications. Increasing the current capabilities of Naval and Marine Corps forces, in a mobile environment, increases the likelihood of enhanced capabilities brought against an adversary. Also, these capabilities can be extended to MIO, VBSS and various missions related to peacekeeping, anti-piracy, fishery, etc. This additional power comes in the forms related to near real-time communications where the front line war fighter or first responder can bring additional capabilities to bear through the use of an interactive communications system capable of providing on-time, accurate and relevant information when absolutely needed.

[12] The term mobile networking refers to a network is mobile and a fixed network that supports mobility.

[13] Mobile networks consist of stationary to moving target communications applications and maritime consists of communications from one moving vessel to another moving vessel.

The mobile networks and future C4ISR systems must also be capable of reaching the GIG or host network and therefore tying in the national assets that allow our forces to fight a global war on terror.

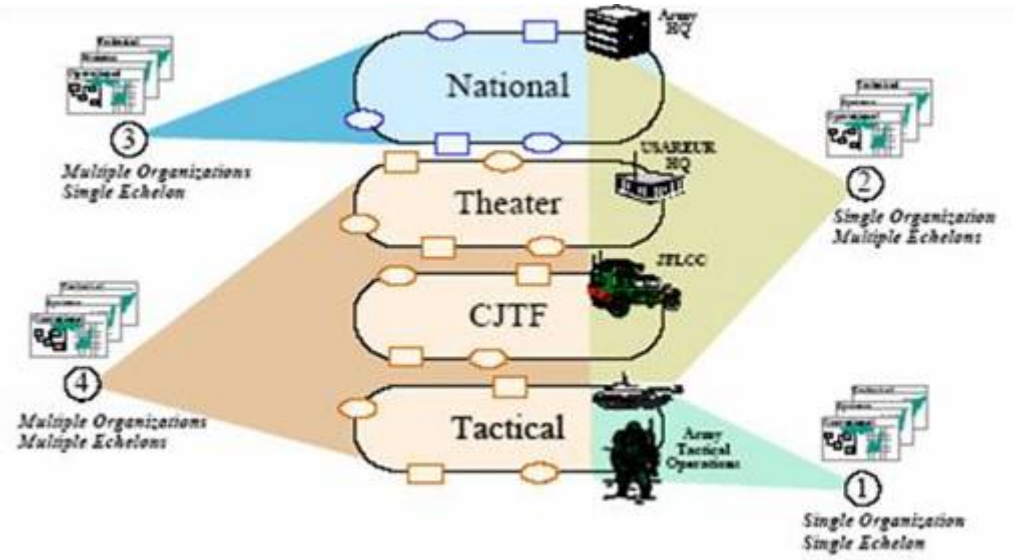


Figure 4. C4ISR Architecture Framework. (From Joint Vision 2010)

This C4ISR diagram shows the framework necessary for future programs and applications that conform to future implementations. Through this framework, future MIOs can tie into these platforms to enhance and augment the information stream necessary to support a MDA strategy.

C. RESEARCH QUESTIONS

The primary question revolves around advancing the technologies of earlier MFLAK operations and how an enhanced communications suite addresses long haul and last mile operations in order to support current MIOs so that boarding officers and commanders have a near real time understanding of ship boarding operations? Additional research can be focused on the following topics:

- Evaluate the impact of this wireless technology on naval communications systems operations with regards to security.

- Analyze and select the system types that could most benefit from this technology.
- Explore how many devices are required to provide persistent coverage for these specific (i.e., sensors, cameras, weather devices, access points, etc.) technologies within a defined Area of Responsibility (AOR)?
- Given wireless connectivity, what types of data can be collected and passed in a real time manner using this technology?

D. SCOPE

The thesis is a system-level test and evaluation of a prototyped ComCase T configuration from Western DataCom. The primary objective of this research was to determine the functional performance envelope and tactical applicability of a network equipped with wireless access points that augment the ComCase technology. To accomplish this objective, a robust test and evaluation plan was produced. Using this test plan, the system was base-lined in the moderate operating conditions of Camp Roberts, California. The system was then tested in various operating environments to include: Fort Hunter-Liggett, California, Fort Ord, California, Indonesia, and Thailand as part of the COASTS 2007 field experimentation program. In addition the system was scheduled to be deployed, tested and evaluated in support of fleet exercises TALISMAN SABER and SEACAT to obtain valuable operational feedback.

E. METHODOLOGY

The research methodology will be conducted in the following phases:

Phase 1: Development of metrics and test plan

This phase will include the necessary academic review of existing technical material for wireless technologies in the 802.16 arena and various mobile devices that include: Biometric equipment, laptops, PDA's, video, etc. Additionally the research will focus on desirable attributes from the end-user's perspective. Measures of Performance and Measures of Effectiveness (MOP/MOE) will be created. The MOP/MOE's will be used to develop an effective test and evaluation plan.

Phase 2: Base-lining and experimentation

Once a test and evaluation plan is created, the MFLAKII system will be base-lined in the moderate operating environment at the Naval Postgraduate School and surrounding areas: specifically, the over-water experimentation shall be conducted with the help of the US Coast Guard operating in Monterey Bay, while the ground and air-based experimentation shall be conducted in the vicinity of Fort Hunter-Liggett, California. The Fortress wireless access point (IEEE 802.11) and the associated software suite has numerous data collection tools built-in. Additional tools such as network analyzers and packet-sniffers (i.e., Netstumbler, Ethereal, IXChariot, etc.) will be utilized.

Phase 3: Analysis of results and conclusions

The final phase consists of analyzing the results of each case study. The results will be compared to the base-lined system. They will also be compared to the MOP/MOE's determined in Phase 1. By comparing the results from the case studies to the base-line and MOP/MOE's, it will be possible to determine the effectiveness and feasibility of deploying the system in real-world military and commercial environments.

F. ORGANIZATION OF THESIS

CHAPTER I

Introduction: This chapter outlines current MIOs and its structure within the Navy's MDA Program. Emphasis shall be placed on the Navy's emerging riverine doctrine[14], as well as, force transformation in special operations commands, modifications of mission requirements and capabilities, communications enhancements and mission's best suited for the Maritime Fly Away Kit (MFLAKII).

CHAPTER II

MDA and MIOs: This chapter will focus on the modern maritime domain and the operations required of coalition forces in that environment. A study of the National

[14] Department of the Navy, Renewal of Navy's Riverine Capability: A Preliminary Examination of Past, Current and Future Capabilities, March 2006.

Security Strategy (NSS), National Maritime Security Strategy (MHLS), and the recently published Quadrennial Defense Report (QDR) will be used to further highlight the requirements of the modern coalition maritime forces. A further study of the history of riverine warfare in the context of the newly established Naval Expeditionary Combat Command (NECC)[15] will be done in order to finalize the C4ISR requirements.

CHAPTER III

Component Selection for MFLAK II: The components gathered from the private sector through vendor relations makes up the majority of the equipment used in the MFLAK and will be detailed in this chapter. IEEE 802.16 D/E OFDM equipment, as well, as the mobile routing, ruggedized component technology and sensor technology will be described, along with explanations of how the MFLAK-II will be integrated into overarching network architecture for NCW. Throughout this chapter, the sensor technologies shall be built to make use of the strengths of the network, while decreasing the form factor necessary to deploy this capability.

CHAPTER IV

Selection of Metrics and Experiment Design: This chapter will focus on the field tests of communications equipment in the MFLAK-II, from the commencement of testing at Camp Roberts, California in November 2006 through the final integrated scenario tests of the completed MFLAK-II in Chiang Mai, Thailand in May 2007. Additional comments shall be added from a variety of tests done in Monterey Bay with the United States Coast Guard in preparation for Talisman Saber 2007 in Brisbane, Australia and EXERCISE SEACAT in the Straits of Malacca. MOE and MOPs will be analyzed to study the performance of the IEEE 802.16 network topology, as well as Ultra-Mobile Computing Devices (UMCD) associated with the MFLAK-II.

CHAPTER V

Maritime Fly Away Kit Generation II: This chapter will be a case study of network-centric warfare in the maritime environment through mobile networking

[15] Navy Expeditionary Combat Command (NECC) stands up in January 2006 to serve as a single functional command to centrally manage current and future readiness, resources, manning, training and equipping of the Navy's expeditionary forces.

translations and protocols and how current technologies could be leveraged to enhance capabilities across the riverine and light vessel communities. This chapter will also focus on how the development of local area networks (LAN), wide area networks (WAN), wireless wide area networks (WWAN) and connecting communications are vital to the integration of NCW.

Additionally, this chapter will discuss the specifications necessary to support Mobile Routing while enhancing the effectiveness of mobile assets in a large scale environment. Lastly, this chapter will address the integration of these capabilities and the technologies necessary to support mobile communications on land and sea.

CHAPTER VI

Conclusions and Recommendations: The culmination of this research will be examined in this chapter. There will be a focus on continued research areas which can be expanded from this thesis upon its completion.

II. MARITIME INTERDICTION OPERATIONS

In order to effectively scope this research endeavor, it is essential to identify the capstone documents that guide to MDA and MIOs. More importantly, these writings offer guidelines and recommendations for transforming existing stakeholders into becoming an integrated force that strives to share data with fellow agencies. By building a "system of systems" it is possible to share the right information at the right time with the right agencies. By empowering these entities at the federal, state and local levels, the reaction time of a first responder decreases and the possibility of thwarting attacks increases.

A. NETWORK CENTRIC WARFARE

Network Centric Warfare is about leveraging information. With this information, it is possible to change the dynamics behind traditional warfare by adapting new modes of operations that allow the information to be transmitted in a near real time scenario. Historically, MIOs were predominantly conducted by a boarding team that collected sensor feeds and data from hands-on contacts. This information was then stored and processed after the actual engagement; perhaps several days later. NCW changes this modus operandi by immediately processing the data into information and then by engaging outside agencies in a near real time scenario that empowers and strengthens the capabilities of the boarding party. Furthermore, the NCW framework enhances combat power that is generated from the effective linking or networking of similar war fighting networks. In this example, the boarding team is capable of receiving relevant and timely information from an adjacent boarding team, miles or countries away, while processing their own mission. This type of cohesion amongst tactical teams gives credibility to the NCW framework and allows various units to leverage this new information capability. This high level sharing leads to heightened battle space awareness that can be exploited via collaborative efforts and other network-centric operations to achieve the commanders' overall intent.

NCW revolves around the information age. More importantly, "NCW recognizes the centrality of information and its potential as a source of power." [16] Net Centric Warfare discusses the Information Age in four different areas[17]:

1. Rate of technological advance, and the ability to turn out new products, has increased dramatically.

2. Advances in technology are being driven by private sector requirements to move and process information on a scale unimaginable just a few years ago.

3. The military is now being driven by a technology cycle that is quickening and has less and less time to react to take advantage of the new capabilities they represent before these, in turn, are overtaken by new capabilities.

4. The pace of technological advances has quickened to such a degree that current DoD methods of incorporating technology are well behind the power curve.

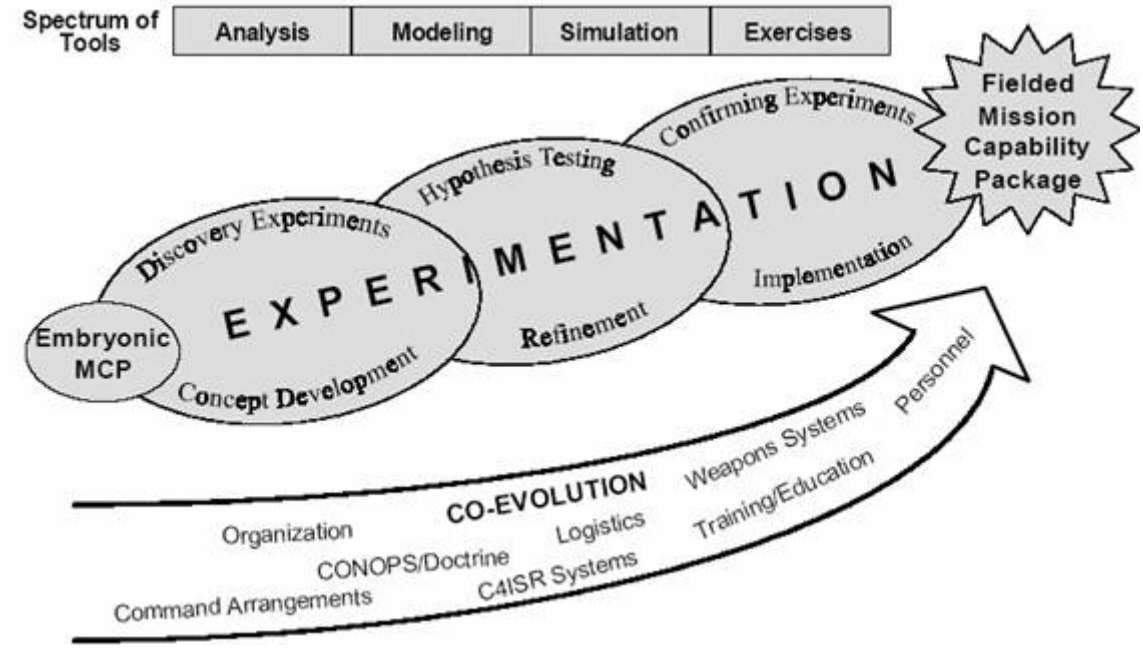


Figure 5. Role of Experimentation in the Co-evolution of MCPs. (From [16])

In Figure 5, NCW has shown that Mission Capability Packages (MCP) can be put into an experimentation environment to assist in the development of the four areas that

[16] David Alberts, et. al.., Net Centric Warfare.

[17] David Alberts, et. al.., Net Centric Warfare 200.

pertain to the Information Age. In Discovery, Hypothesis Testing and Confirmation, a MCP can be implemented that effectively changes the way traditional systems evolve. For example, the COASTS effort embodies these four principles by nurturing a program based almost primarily on the experimentation of COTS equipment. Coincidentally, COASTS' experiments follow the Co-evolution of MCPs and aid in the identification and development of technological advances available through commercial means and adapted for military operations. COASTS is capable of developing, refining and implementing COTS equipment. This is done through test labs, field experimentation and military exercise engagements that validate the findings within the COASTS program. Although COASTS does not address all components of MCP, it does specifically focus on Infostructure Systems.[18]

"Infostructure systems will provide key capabilities (bandwidth, processing power, stored information, decision aids, and agents) and need to be better designed to support battle space entities as they interact much more closely than ever before."[19] These Infostructures focus on sensors and intelligent data sources to provide the information capable of empowering the war fighter. Their job is to provide data or information conforming to the "timely, accurate and relevant" mantra that surrounds Information Warfare. In supplanting legacy systems, 21st century networks empower tactical units by providing increased situational awareness, greater throughput capacities for higher bandwidth applications and quality information that has been processed and delivered at the appropriate time. Thus, the legacy systems and the individual systems available today have become obsolete if they are not capable of joining the network and conforming to the framework in NCW. Unfortunately, the NCW framework demands a test platform that closely emulates the real world environment without actually putting the war fighters on the front line of evaluating the equipment. Ultimately, COASTS type programs must grow within the NCW framework and continue to contribute to the MCP's and other areas in order to closely resemble today's current operating forces. In

[18] Information Infrastructure, term coined in Alberts' Net Centric Warfare.

turn, this will decrease the burden placed on operational units to field R&D technologies and, instead, use programs that emulate their environment in order to provide a simulated operational unit.

In the NCW framework, we must also focus on Virtual organizations[20] that bring the people and processes together to accomplish a particular task. When the task is over, these resources can be released for other tasks. Virtual organizations make location less important and the opportunities for collaboration, integration, and outsourcing more beneficial. For example, within the COASTS program, the ESP Group provides a secure portal that is based on Virtual organizations. To further delve into this example, the portal is activated for a specific operation where several subject matter experts (SME) from around the world are asked to weigh in on current operations in a given AOR. Collaboratively and virtually, this group meets in real time to discuss the possible solutions and remedies for the current set of problems (see Figure 6). Once the problems and scenarios are complete, the SME's are returned back to their respective work environments.

[19] David Alberts, et. al.., NCW 195.

[20] Virtual organizations allow enterprises to take advantage of the potential gains in productivity that are associated with virtual collaboration, virtual integration, and outsourcing. NCW page 111.

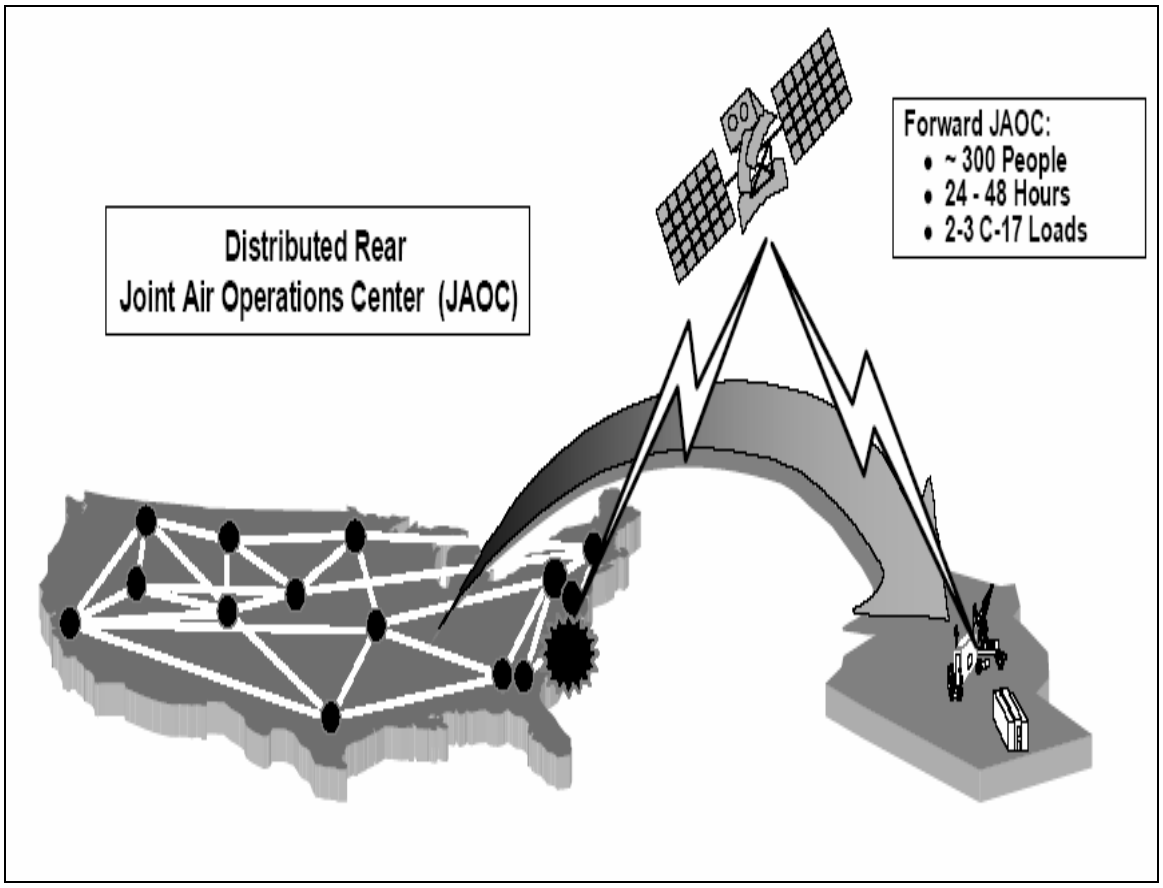


Figure 6. Virtual Collaboration—Moving Information, Not People. (From [21])

B. NATIONAL STRATEGY FOR MARITIME SECURITY

Achieving Domain Awareness in the maritime environment is a challenging task. "The heart of the MDA Program is accurate information, intelligence, surveillance, and reconnaissance of all vessels, cargo, and people extending well beyond our traditional maritime boundaries."[22] Domain awareness enables the early identification of potential threats and enhances appropriate responses. The vastness of the earth's littorals combined with the real world threats, imagined and unimagined, do not bode well for our nations defenders. The international waters are not regulated and the "registration and ownership of vessels and cargoes, as well as the fluid nature of the crewing and

[21] David Albert, et. al., Network Centric Warfare 111.

[22] President George W. Bush, January 2002.

operational activities of most vessels, offer additional opportunities for concealment and challenges for those attempting to maintain maritime security."[23] The modern forces must be capable of integration and information sharing through the various federal, state, local and coalition agencies. It is dependent on the ability or our sensors to collect data and correctly parse the information and catalogue it for dissemination as appropriate. To maximize domain awareness the United States leverages its global maritime intelligence capability and the diverse expertise of the intelligence and law enforcement communities. Similarly, COASTS uses the integrated Common Operational Picture (iCOP)[24] to collect, fuse, integrate, and disseminate timely intelligence and information. Through this platform it is possible to collect data, fuse it with relevant services, integrate it into a common picture and disseminate it across a global network. By performing these operations, the Information Age leverages the four areas of Net Centric Warfare and guides off of the National Security Strategy for Maritime Security. Additionally, the Department of Homeland Security oversees the implementation of a shared situational awareness capability that integrates intelligence, surveillance, reconnaissance, navigation systems, and other operational information inputs, combined with multiple levels throughout the United States Government.

C. DEPARTMENT OF HOMELAND SECURITY

The DHS[25] was established through The National Strategy for Homeland Security in 2002. It aligns and focuses homeland security functions into six critical mission areas: intelligence and warning, border and transportation security, domestic counterterrorism, protecting critical infrastructure and key assets, defending against catastrophic terrorism, and emergency preparedness and response. The first three mission areas focus primarily on preventing terrorist attacks; the next two on reducing our Nation's vulnerabilities; and the final one on minimizing the damage and recovering from attacks that do occur.[26]

---

[23] Department of Defense, National Security Strategy on Maritime Security, 19.

[24] Vector Relational Database Model (VRDM).

[25] Homeland security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. National Strategy on Homeland Security, page 14.

[26] Department of Homeland Security, National Strategy on Homeland Security, 16.

For Fiscal Year 2003, President Bush requested a significant increase in homeland security research and development funding. The increase from $1 billion to $3 billion identified several major initiatives that must be addressed in terms of Science and Technology:[27]

- Develop chemical, biological, radiological, and nuclear countermeasures.
- Develop systems for detecting hostile intent.
- Apply biometric technology to identification devices.
- Improve the technical capabilities of first responders.
- Coordinate research and development of the homeland security apparatus.
- Establish a national laboratory for homeland security.
- Solicit independent and private analysis for science and technology research.
- Establish a mechanism for rapidly producing prototypes.
- Conduct demonstrations and pilot deployments.
- Establish a system for high-risk, high-payoff homeland security research.

These initiatives are crucial in identifying long-term research programs that are capable of revolutionary changes in DHS.

From the above listed initiatives, COASTS presents a program that addresses and confronts these issues. Some of COASTS' goals for 2007 included the introduction of new technologies such as recent advances in wireless networking and biometric data gathering, improved C4ISR sensors and the new UAV capabilities. These goals are in line with DHS' systems for detecting hostile intent, biometric technologies, and improved technical capabilities of first responders, rapid prototyping and the conduct of demonstration and pilot deployments. Throughout 2007, COASTS has led several experiments with the United States Coast Guard and Royal Thai Air Force, as well as, briefed DHS and senior Coast Guard officials about projects and partnerships that address these initiatives.

[27] Department of Homeland Security, National Strategy on Homeland Security, 52.

D. COASTS

COASTS is a combined Indonesia-Malaysia-Singapore-Greece-Thailand-U.S. Research and Development (R&D) effort to investigate commercial-off-the-shelf (COTS) Command and Control, Communications Computers and Intelligence, Surveillance and Reconnaissance (C4ISR) technologies to provide real-time situational awareness (SA) for multi-national, tactical and remote decision makers in a cooperative environment. COASTS-07 is the third iteration in the series and will build on the successes and lessons learned from the 2005 and 2006 field experiments. Moreover, COASTS 2007 expanded the scope of the 2006 field experiments. A broader geographic area was utilized, several more U.S. and international partners were included and additional technologies and their associated commercial companies were leveraged. In 2007, COASTS employed select technologies into two major multi-national Pacific Fleet exercises, specifically US Pacific Fleet's exercise TALISMAN SABER 2007 in Australia during June 2007 and COMLOG WESTPAC's Southeast Asia Cooperation Against Terrorism (SEACAT) 2007 exercise in Singapore on August 2007.

The COASTS 2007 vision incorporates international and domestic partners at the R&D level through cooperative Science & Technology (S&T) field experimentation. Operating at the R&D level allows COASTS to be more efficient without the many added requirements associated with traditional military-to-military engagement.

Specifically, COASTS-07 objectives included:

- Investigating net-centric information management in multi-national environments across tactical, operational, and strategic domains
- Make ISR data and information visible, available and usable when and where needed
- Create synergy with the US Pacific Command's (USPACOM) Theater Security Cooperation Plan and supporting theater objectives (long-term influence)
- Expand the scope of MDA and protection research into improved command and control (C2) technologies for Maritime Security Operations (MSO)

• Demonstrate ship-to-ship and ship-to-shore communication capabilities in deployable form factors

• Investigate deployment issues surrounding hastily formed networks in rugged and varied terrain under adverse climatic conditions

• Investigate the utility of mini-UAVs and sensor suites in rainforest, littoral, and maritime environments

• Investigate integration issues surrounding non-governmental organization (NGO) and international partner participation

• Investigate the dissemination, parsing, protection, security, and sharing of information between various U.S., international, and commercial partners

• Partner with USPACOM, COMPACFLT and COMSEVENTHFLT to integrate selected COASTS technologies into exercise TALISMAN SABER-07

• Partner with COMLOG WESTPAC to integrate selected COASTS technologies into exercise SEACAT-07.

Achieving these objectives improved command and control support for friendly assets, disadvantaged users, and tactical units in support of maritime and littoral missions. The COASTS operational goals provided training and support refinement of TTPs and CONOPS for combined and interagency forces conducting several principal missions: force protection, tactical surveillance and reconnaissance, internal defense, combating terrorism and transnational crime, civil affairs, counter-proliferation of weapons of mass destruction, information operations, maritime security, and MIOs.

The phased spiral development that proved successful in 2006 was refined for COASTS-07. Initial phases early in the fiscal year were limited to reduced-scale baseline deployable architectures designed and tested in CONUS locations. Follow-on phases provided tailored benchmarking and opportunities to optimize system performance in the more challenging OCONUS environments. Finally, the complete COASTS system architecture was deployed and the operational demonstrations were conducted with great success. These approaches reduced technical risk by verifying that the new technologies were configured and integrated to function in the intended environments.

THIS PAGE INTENTIONALLY LEFT BLANK

III. COMPONENT SELECTION FOR MFLAK II

A. MISSION

In approaching NCW and MCP's for the future, the trend toward linking units and personnel through the use of Internet Protocol (IP) has arisen. This capability demands a rugged, small form factor and scalable solution that meets the demands put forth in NCW and the information sharing domain. After the writing of RFC 3344[28] (Mobile IP for IPv4), commercial companies have been developing and prototyping equipment capable of supporting a mobile IP network and pushing it to the lowest echelon of tactical units, first responders and assorted personnel. To be successful in this implementation, the equipment must support roaming and mobile networks at various speeds, altitudes and environments (e.g., land, air, sea, etc.).

In designing a next generation Fly Away Kit, the conceptual design mandated that form factor and mobility were key attributes in developing a second generation product. By moving from rack mountable units to configurable, small, kitted units, the end user has the ability to configure as appropriate. Additional parameters considered included power consumption and longevity, ruggedization, portability, range and adaptability.

Ultimately, the use of Mobile IP was primed for deployment and was successfully demonstrated in multiple exercises on various platforms. From the end user, to the vehicle, to the aircraft or the ship, Mobile IP proved rugged enough across all platforms and performed the various missions with excellent results.

In testing and integrating the next generation Fly Away Kit, the COASTS-07 program was used to design, test and demonstrate the scalability, applicability and robustness of the network. The scenarios in COASTS (see Appendix E) assisted the mobile IP testing/implementation by controlling specific portions of the exercise. For example, the Maritime Interdiction scenario allowed the research team to focus on ship-to-ship communications and protocol handoffs while supporting the end user in

[28] RFC 3344 (Aug 2002) supersedes RFC 3220 (Jan 2002) and RFC 2002 (Oct 1996) respectively.

transmitting data through the network to a local command and control center referred to as the COASTS Tactical Operations Center. By using a test plan, augmented by a scripted scenario, the testing proved successful by supporting the end users with the time necessary to troubleshoot and implement various changes in this dynamic atmosphere. The following in an excerpted figure from "PC/104 and Small Form Factors" article citing net-centric operations and provides a possible scenario for mobile IP applications.

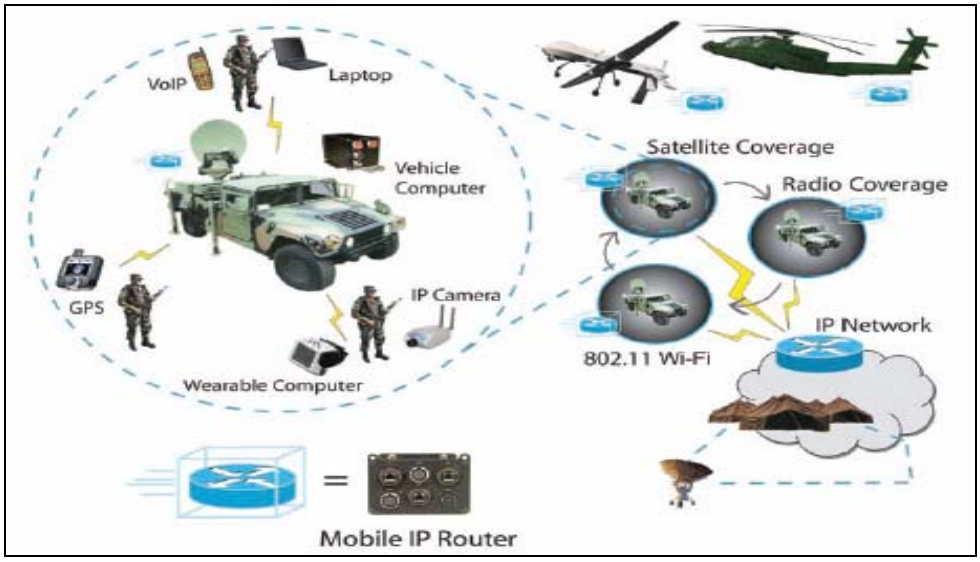


Figure 7. Mobile nodes roaming across multiple networks. (From www.cisco.com)

This overview provides segues into the technologies based on mobile IP technologies and creates the foundation for a next generation Maritime Fly Away Kit.

B. TOPOLOGY

1. COASTS 2006 Background

The goal of the COASTS-06 network was to build and demonstrate the flexibility, mobility, durability, and scalability of COTS IEEE 802.11 a/b/g and IEEE 802.16 wireless networks deployed to rugged and varied terrain under adverse climatic conditions. These networks were the infrastructure for transmitting state of the art sensor and ISR data providing improved tracking of littoral and ground movements, identifying

which tracks were potential threats, prioritizing them for action, and providing engagement confirmation and battle damage assessment.

The COASTS-06 network was designed to be robust, rapidly deployable, modular, and reconfigurable to meet all the needs of tactical, operational, theater, and strategic decision makers in coalition environments. COTS technologies, in particular open standard/open source technologies, provided these capabilities due to their ease of configuration, small form factor, technological proliferation, and low cost.

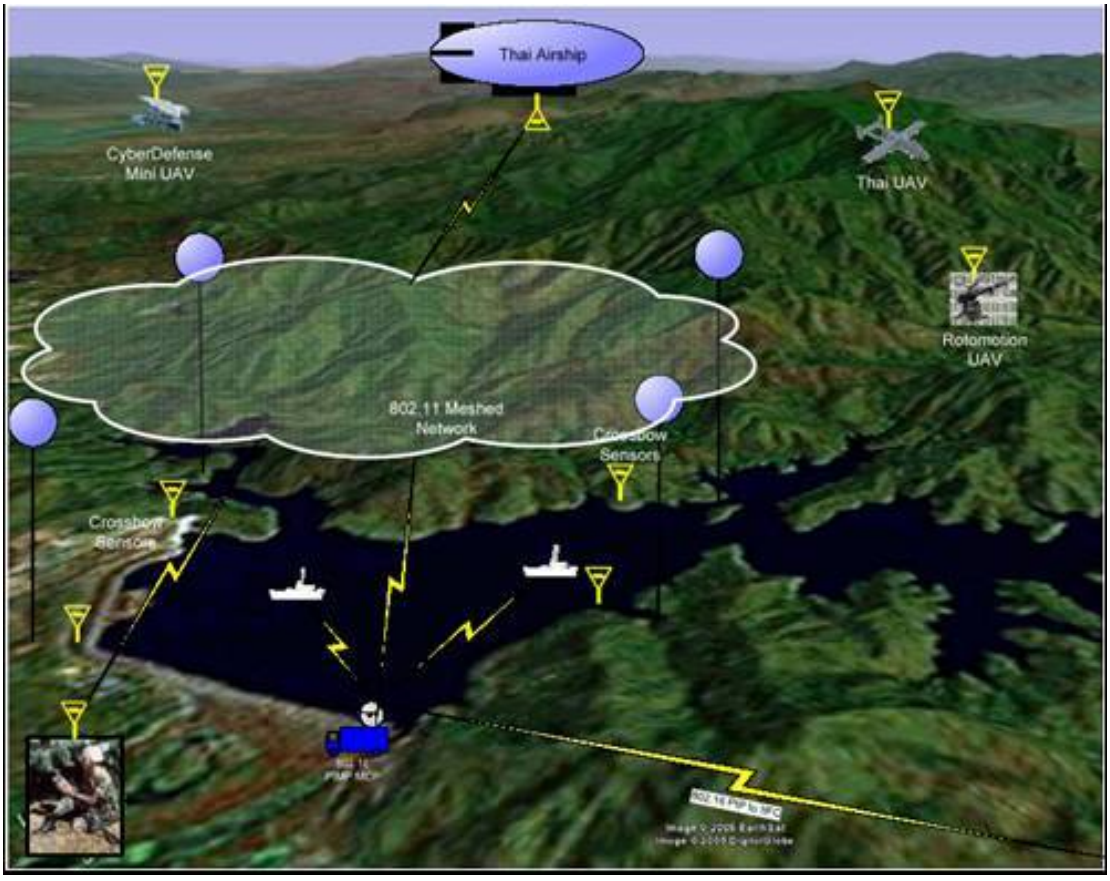


Figure 8. COASTS Topology 2006.

2. COASTS 2007 Background

COASTS goals for 2007 include the introduction of new technologies such as recent advances in wireless networking, mobile IP, and biometric data gathering, improved C4ISR sensors and new UAV capabilities. Many lessons learned from 2006

were addressed. These include longer life and more robust power supplies for all network nodes and optimization of network design for true “plug and fight” interoperability with appropriate security.

The operational goals provided training and supported refinement of TTPs and CONOPS for combined and interagency forces which conducted several principal missions: force protection, tactical surveillance and reconnaissance, internal defense, combating terrorism and transnational crime, civil affairs, counter-proliferation of weapons of mass destruction, information operations, maritime security, and MIOs. COASTS technologies were intended for use by individual and small units and are solely based on a mobile network environment. The principal systems are annotated in Figure 9 and include:

- Wireless network communications systems
- Simple Network Management Protocol (SNMP) based multi-sensor networking devices
- Networked sensors
- Biometric systems
- UAVs (fixed and rotary wing)
- Tethered balloons
- Portable computing systems
- C4I software applications
- Deployable meteorological and oceanographic (METOC) sensor suites
- Information management portals

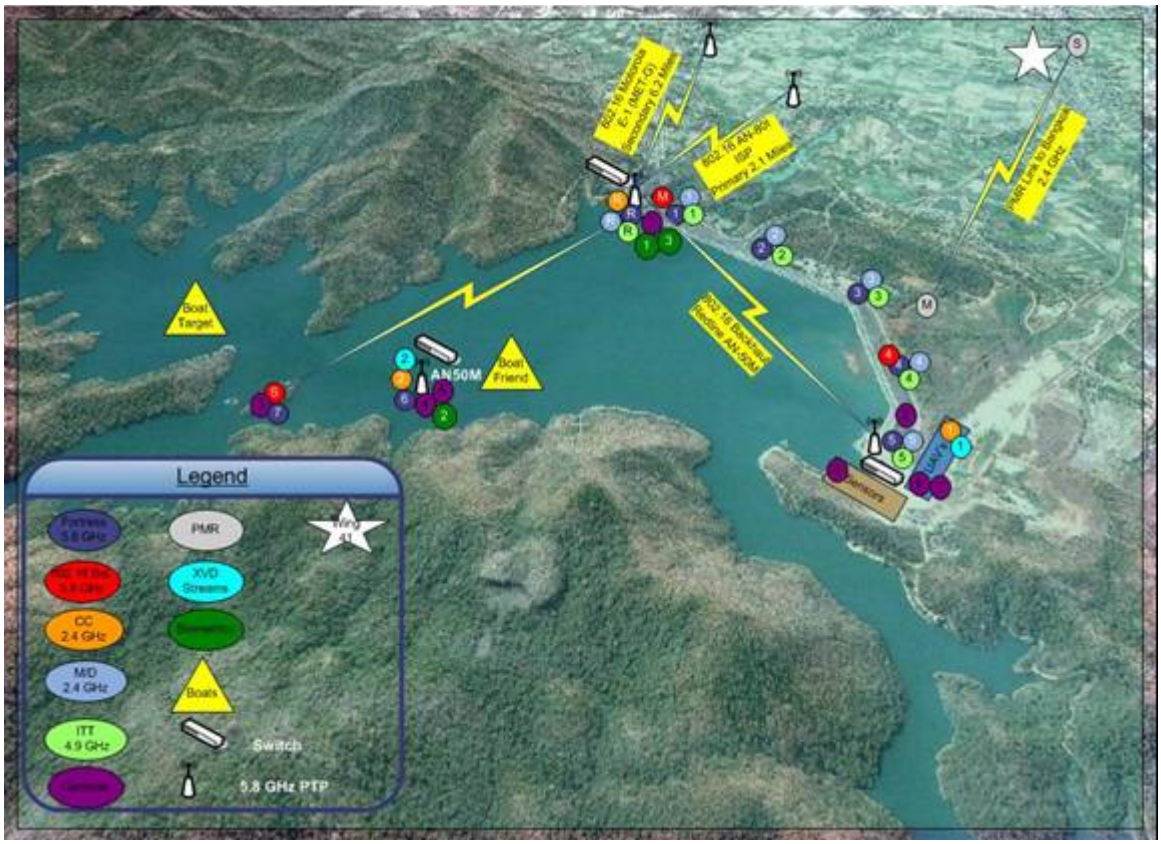


Figure 9. COASTS 2007 Topology.

C. MOBILE COMPUTING

Mobile Computing is increasingly important in terms of the number of mobile users currently using cell phones, PDA's, Bluetooth devices and other wireless computing devices. Since the Internet is based around the TCP/IP layers of the OSI model, there is a direct tie between cellular and mobile networks. Currently, the Internet Engineering Task Force (IETF) addresses mobile computing through RFC 3344[29]. Mobile IP supports the Mobile computing concept and is designed to allow each mobile router on the network to have two IP addresses. One of the IP addresses is the permanent home address that is assigned at the home network. The other is a temporary "care-of"[30] address that represents the current location of the host. The main goals of Mobile IP are

[29] RFC 3344, August 2002, IP Mobility Support for IPv4.

[30] The IP address of the mobile networks' current point of attachment to the Internet.

to make mobility transparent to the higher level protocols and to make minimum changes to the existing infrastructure.

In mobile networking, a mobile node must be able to perform the following functions:

- Communicate with other nodes after changing its link-layer connection to the Internet, but not changing its IP address.
- As an architectural constraint, it must be backwards compatible with nodes that do not have mobile routing.
- As an architectural constraint, no changes to original protocol structure are required in hosts or routers that are not acting as any of the new architectural entities.
- Messages from mobile nodes must be authenticated to deter redirection attacks.
- Move from one IP subnet to another IP subnet without losing connection.
    - This change can be done from wireless to Ethernet or vice versa.[31]

There are two kinds of relationships in Mobile IP:

- A home agent stores information about mobile nodes whose permanent address is in the home agent's network.
- A foreign agent stores information about mobile nodes visiting its network. Foreign agents also advertise care-of addresses, which are used by Mobile IP.

A node wanting to communicate with the mobile node uses the home address of the mobile node to send packets. These packets are intercepted by the home agent, which uses a table and tunnels the packets to the mobile node's care-of address with a new IP header, preserving the original IP header. The packets are decapsulated at the end of the tunnel to remove the added IP header and delivered to the mobile node.

When acting as sender, mobile node simply sends packets directly to the other communicating node through the foreign agent. If needed, the foreign agent could employ reverse tunneling by tunneling mobile node's packets to the home agent, which in turn forwards them to the communicating node.

[31] RFC 3344.

1. Routing Equipment

COASTS-07 leveraged mobile IP through the use of multiple routing devices. This enabled the COASTS architecture to abandon classic rack mounted components and switch to mobile devices capable of roaming, wired and wireless connections. The following list of equipment outlines the components used in the development of the MFLAK-II.

Western DataCom offers several lines of Mobile Routers and COASTS-07 used the ComCase T, ComCase H and Grizzly configurations to support mobile network operations in air, on land and at sea. The ComCase E and G were analyzed, but not used in any field experiments.

a. ComCase T

The ComCase T was selected as the primary component for the TOC. It provided a small form factor, multiple serial interface ports for router connections, a wireless access point and a server for network applications. It provided a rugged, small form factor, MIL-STD 810F[32], portable solution utilizing mobile IP. The ComCase T provided IEEE 802.11 a/b/g wireless bridging/access point and was also used with cellular modems that were capable of operating on Verizon, Sprint, Cingular and T Mobile nationwide networks. Additionally, the ComCase T used an Intelligent Video Server that was capable of multicasting and unicasting dual video feeds. As a small form factor, 9.75"w x 10"h x 15"d and weighing less than 26 pounds, the ComCase T was easily transported through multiple moving vehicle scenarios and shipboard operations. Its fan-less design eliminated concerns of dust and water while dissipating heat through the thermal plate heat dissipaters. The ComCase T was equipped with the Cisco 3200 Series router which created an IP network for the vehicle, enabling secure voice, video, and data communications with the TOC. The vehicle network maintains seamless connectivity while stationary or in motion by utilizing mobile internet protocols.

[32] MIL-STD-810 series of standards are issued by the United States Army's Developmental Test Command, to prove that equipment qualified to the standard will survive in the field.

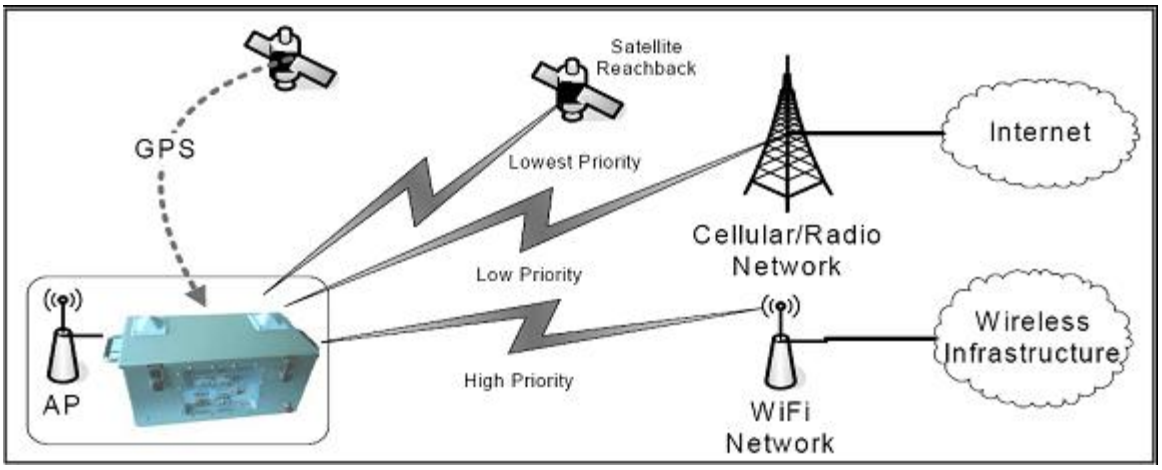


Figure 10. ComCase T from Technical Brochure. (From www.westerndata.com)

b. ComCase G

The ComCase G was not selected, but was considered during trials and may prove to be of future use in further iterations that support pole mounted routers. The ComCase G is a rugged form factor, MIL-STD 810F, pole mountable solution utilizing the Cisco 3200 Series Wireless and Mobile Router including the Cisco WMIC for Cisco 3200 Series Routers. The ComCase G had a 14 slot aluminum enclosure that included an integrated AC-DC power supply for connection directly to AC power sources from 85 to 264VAC. The ComCase G is NEMA-6[33] approved, maintains emissions and safety approvals and has been tested to the most stringent environmental standards. Its rugged, fan less design eliminates concerns of dust and water. All inlets and outlets are gasketed, watertight and the enclosure is totally sealed to outside elements. Easy access is provided via the protective end cap cover which opens 180 degrees.

c. ComCase E

The ComCase E was not selected, but was considered during trials and may prove to be of future use in further iterations that disaster recovery scenarios or continuity plans. The ComCase E includes all the components necessary to operate a mobile IP based application, to include IEEE 802.11 a/b/g and cellular modems that are

[33] All NEMA 6 devices are three-wire grounding devices used for 208V and 240V circuits and rated for 250V maximum.

capable of operating on Verizon, Sprint, Cingular and T Mobile nationwide networks. In addition it supports the IPE-10M[34] for securing mobile communications using 256-bit AES counter mode encryption. The ComCase E used only approved components and was designed for rugged travel applications. It measures 5"w x 12"h x 12"d.

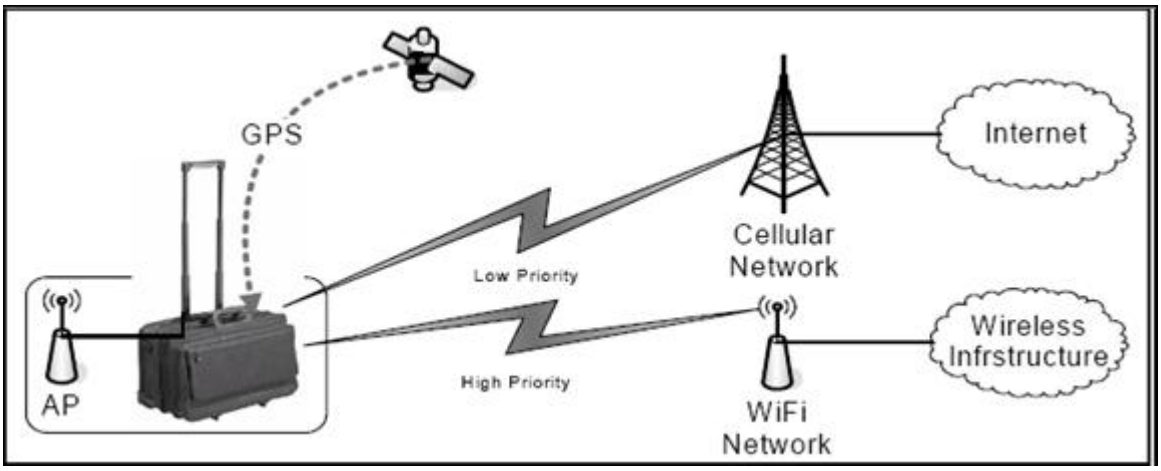


Figure 11. ComCase E from technical brochure. (From www.westerndata.com)

d. ComCase H

The ComCase H was used in scenario tests during mobile vehicle simulations. It proved to be cumbersome in mobile applications, but may be beneficial in TOC/NOC scenarios. The ComCase H allowed forward deployed combatants and first responder incident commanders to maintain situational awareness and command while in a mobile status. ComCase H has rugged MIL-STD 810F chassis components providing portable mobile Internet Protocol (IP). The main IP component is the Cisco 3200 Mobile Access Router (MAR) using the IETF standard RFC 3344 for Mobile IP. The MAR provided an integrated IEEE 802.11 b/g wireless capability and automatically switches to WiFi bridging, cellular, radio or satellite reach-back[35] to their home station operations

[34] The IPE-10M is a PC/104 Plus High Assurance IPsec Encryptor. Using hardware based security, the IPE-10M is designed to secure all private/public IP internetworking environments (mobile, wireless, space and stationary).

[35] Not used for COASTS-07 but planned for COASTS-08 through a PC/104 VSAT card.

network. Radio over IP, VoIP and Video applications allowed team members the ability to have inter– and intra– group voice communications and data sharing capabilities.

The ComCase H had MIL-STD 810F Chassis Components and a Tablet PC with Wireless MIL-STD 810F Keyboard, Portable Form Factor with Tie Downs and Carry Handles, Militarized External Interface Connectors and a 1W IEEE 802.11b/g Amplifier with Diversity WiFi Omni Antennas[36].

The ComCase H supported Western DataCom's Intelligent Video Server (IVS) and Digital Video Recorder (DVR) for video surveillance applications. The Cisco IP Interoperability and Collaborations Systems (IPICS) that allows Radio interoperability (RoIP) was also supported in this chassis but not used during the exercises. All inlets and outlets of the ComCase H are gasketed and watertight, sealing out outside elements, thereby eliminating concerns of dust and water. The ComCase H came with lockable lids that provided for easy access, while measuring 9.75"w x 10"h x 15"d and weighing 35 pounds.

Figure 12. COMCASE H ROUTER from Technical Specifications. (From www.westerndata.com)

[36] Diversity is the spatial coding techniques for a Multiple In / Multiple Out (MIMO) system in wireless channels.

e. Grizzly

The Grizzly was chosen for its small form factor, durability and ability to serve mobile routing and IVS protocols. The Cisco 3200 Rugged Chassis is a fully integrated Cisco Mobile Access Router in a rugged MIL-STD-810F approved chassis. It includes all the components necessary to operate a mobile IP based application. The 3200 Rugged Chassis had an integrated cellular modem that was capable of operating on Verizon, Sprint, Alltel, Cingular and T Mobile nationwide networks. The Grizzly used only approved components and was designed to dissipate heat through passive conduction using custom designed thermal plates. Passive conduction meant the 3200 rugged chassis did not require fans to maintain a consistent operating temperature.

Also incorporated in the Grizzly was the Intelligent Video Server (IVS) PC/104 Card with Mango DSP multimedia platform specifically targeted for the Cisco 3200 Series Wireless and Mobile Router. The IVS was ideal for surveillance in addition to other video streaming applications. The IVS was a PC/104 card designed for low power, rugged, mobile and stationary applications. The TI DM642 DSP processor allowed the IVS to deliver MPEG4[37] compressed video stream at 4CIF[38] resolution 704x480 pixels at up to 30 frames per second (FPS). Video is streamed over the onboard Ethernet interface using industry standard RTP/RTSP.[39] The IVS supports audio and video output for applications such as intercom and video decoding. The DSP processor provided an intelligent means for efficiency at the edge adaptive bandwidth control. The IVS utilizes video analytics software from ObjectVideo, which allowed it to detect and classify such objects as people, unwanted activity and vehicles based on user defined rules. Backend server architecture provided an easy to use graphical management interface to rapidly control rules and alerts. The Grizzly measures 6” x 7” x 8” and weighs 15 pounds.

---

[37] MPEG-4 is a standard used primarily to compress audio and visual digital data.

[38] Common Intermediate Format (4xCIF) is used to standardize the horizontal and vertical resolution in pixels of YCbCr sequences in video signals.

[39] The Real Time Streaming Protocol (RTSP) is a protocol for use in streaming media systems which allows a client to remotely control a streaming media server, issuing commands such as "play" and "pause,” and allowing time-based access to files on a server.

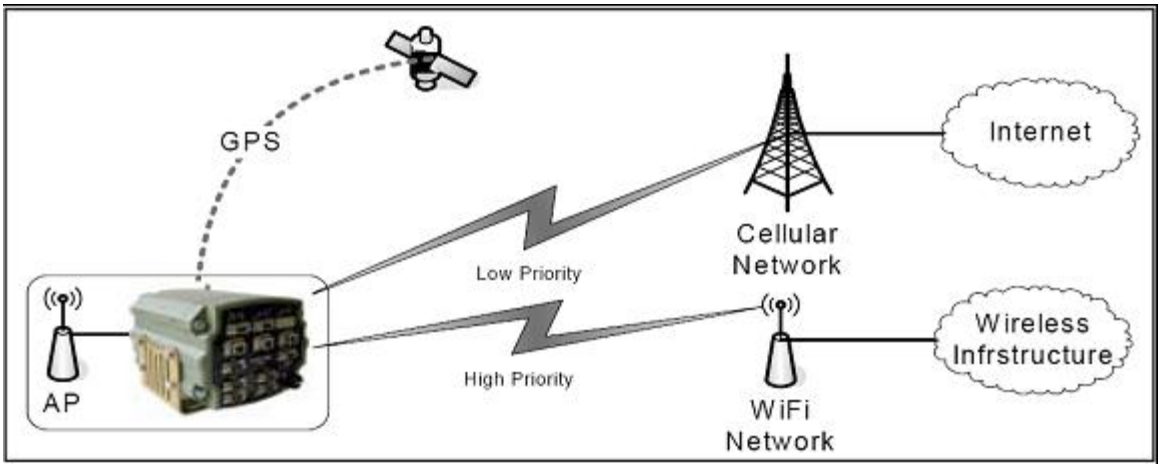


Figure 13. Grizzly from Technical Brochure. (From www.westerndata.com)

2. IEEE 802.11 AND 802.16 PRODUCTS FOR CONNECTION AND BACKHAUL

For COASTS-07, the majority of the back haul was completed using the IEEE 802.16 standard. WLAN's utilized the IEEE 802.11 a/b/g standards.

The IEEE 802.16 protocol, also known as the Worldwide Interoperability for Microwave Access (WiMAX), deals with broadband wireless access. The forum that manages IEEE 802.16 began developing technologies for wireless metropolitan networks in 2000 and published its first standard in April 2002 for equipment operating in the 10-66 GHz frequency band.[40] Fortunately, the group extended the standard (IEEE 802.16a) for use in the lower frequency range of 2-11 GHz. This new frequency range allows for non-line-of-sight connectivity. The current standard IEEE 802.16-2004[41] deals specifically with wireless connectivity between fixed devices. In addition, a new mobile standard (IEEE 802.16e) is currently under development that would allow access via portable devices such as laptops, personal digital assistants (PDA) and mobile phones. The fixed and mobile standards have evolved separately due to the complexity of mobile handoffs from one cell to another. Finally, one of the new task groups (IEEE 802.16f) is working on incorporating mesh networking capabilities into the standard. If it succeeds this could extend the range of networks by allowing each cell in the network to backhaul

[40] IEEE 802.16 Working group.

[41] Previously IEEE 802.16d.

traffic from other cells, effectively routing around obstacles such as mountains. An amendment to IEEE 802.16-2004, IEEE 802.16e-2005[42], addressing mobility, was concluded in 2005. This implemented a number of enhancements to IEEE 802.16-2004, including better support for Quality of Service (QoS) and the use of Scalable OFDMA, and is sometimes called "Mobile WiMAX," after the WiMAX forum for interoperability.

a. Redline AN-80i IEEE 802.16 Radio Transmitter

The AN-80i was selected for its backhaul capabilities for medium to long distances and high throughput rates. It was an IEEE 802.16 compliant, high-performance, high-speed wireless Ethernet bridge for use in commercial, industrial, business, or government environments. The system operated in the 5.8 GHz band using a time division duplexing (TDD) Radio Frequency (RF) transceiver to transmit and receive on the same RF channel. The AN-80i features include: advanced technologies to address inter-cell interference, enhanced security features through a proprietary over-the-air encryption scheme, and Automatic Transmitter Power Control (ATPC) to automatically achieve and maintain optimum performance.

The AN-80i outdoor unit, used for COASTS-07, was housed in a weatherproof aluminum alloy case. The outdoor unit was used with a selection of external antennas which is discussed in greater detail later in the next chapter. When equipped with a narrow beam antenna, the AN-80i was capable of supporting long-range operations over 50 miles in clear line of sight (LOS) conditions with 108 Mbps of throughput. For power, the AN80i uses the Power over Ethernet (PoE) feature. PoE utilizes a module that inserts DC voltage into the unused wires in a standard Ethernet cable (generally pairs 7-8 and 4-5). This is done to supply the powered devices power and UTP Ethernet connectivity requirements via a single Ethernet cable. This proved to be a significant advantage during the sea trials when electrical power was not always available for use where the AN-80i was installed.

[42] Previously known as IEEE 802.16e.

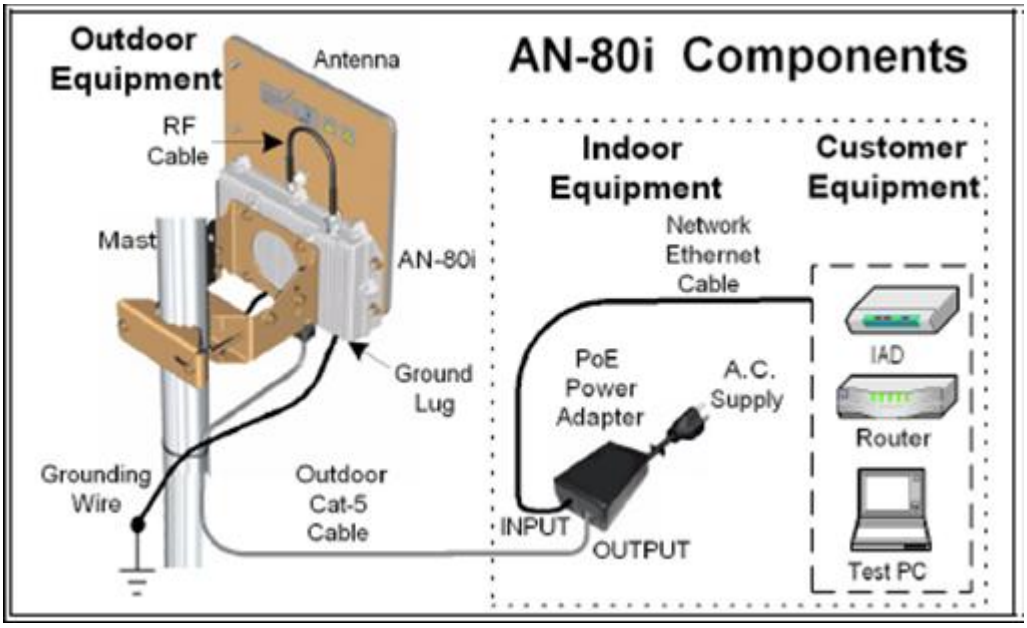


Figure 14. Redline AN-80i - IEEE 802.16 Radio Transmitter Setup. (From AN-80i User Manual)

b. Motorola Spectra PTP 600 IEEE 802.16 MIMO Radio Transmitter

The Motorola 600 was selected for its longhaul capabilities and dual radio technology which supported large bandwidth requirements over long distances. The Motorola 600 Series point-to-point radio operates in the 5.4 GHz and 5.8 GHz ranges. Wireless Ethernet bridges provide more range and capacity in near- and non-line-of-sight (NLoS) environments, delivering high availability wireless communications with network availability approaching 100% even in severe conditions (i.e., high heat, high humidity, raining, snowing, freezing). The Motorola Spectra combines Multiple-Input / Multiple-Output (MIMO) and Intelligent Orthogonal Frequency Division Multiplexing (iOFDM) with advanced signal-processing algorithms, allowing the 600 Series solutions to create four simultaneous signals between pairs of transceivers at each end of the link – without losing spectrum efficiency. By testing the channel spacing through a spectrum analyzer, it was confirmed that the channel size was 30 MHz and the tested throughput was capable of 300 Mbps. The Motorola Spectra was equipped with T1/E1 ports which could have been used to handle circuit switched connections. It measures 11” x 11” x 3” and weighs 9 pounds.

Data security over the wireless link provided by the Motorola 600 series was provided by a proprietary AES 128 and 256 encryption scheme which were contained in the radios. The algorithm used by the 600 series was FIPS-197[43] accredited.

Figure 15. Motorola PTP 600 Tech Specifications. (From Motorola PTP600 User Manual)

c. Fortress ES-520 IEEE 802.11 Radio Transmitter

Fortress provided FIPS and JITC validated integrated wireless security network solutions (ES520), as well as the overlay solutions (FC-X) which encrypted all infrastructure network topologies during the COASTS-07 field tests and experiments. The Fortress ES520 device is lightweight (about 3.5 lbs.). This allowed for the ES520 to be easily mounted high on the light poles which significantly reduced signal loss through cable and resulted in much farther radio range than when they were mounted on ground structures. The Fortress ES520 included (8) 10/100 Megabit switch ports which provided a convenient means to stream video and collect data at remote locations. The ES-520 utilized PoE while mounted on light poles, in aircraft, ships and roving vehicles.

[43] FIPS approved: AES under the FIPS 140 standard.

d. Cisco 2.4GHz Wireless Mobile Interface Card (WMIC) IEEE 802.11 Radio Transmitter

The Cisco 2.4 GHz, IEEE 802.11b/g Wireless Mobile Interface Card (WMIC) for Cisco 3200 Series routers provided IEEE 802.11b/g wireless LAN capabilities during COASTS-07 exercises. Designed in the same ruggedized, compact PC/104-Plus form factor as the Cisco 3200 Series Router, the Cisco 2.4 GHz IEEE 802.11 WMIC was engineered to be integrated as part of a Cisco 3200 Series Router solution, eliminating the need to use external IEEE 802.11b/g bridges or access points. The integrated WMIC helped enable the mobile network in aircraft, vessels, vehicles and garrison networks around the Tactical Operations Center (TOC).

Figure 16. Cisco 3200 Wireless and Mobile Router with 2.4 GHz IEEE 802.11b/g WMIC. (From www.westerndata.com)

3. NETWORK SECURITY

Network security was handled in a variety of ways during COASTS-07. For security concerns on the network, COASTS-07 employed a three-tiered approach: Network Access, Authentication and Validation. *Network Access* was the process of authentication and validation of your computer required for network access. This was done by controlling the use of the Fortress Secure Client Version 4. Prior to receiving the Fort Secure Client, all participants requesting access to the network registered using the

Bio-Pen signature verification mechanism before being granted permission to use the Fortress Secure Client. *Authentication* was the process of verifying your access to the network by confirming your username and password and associating it with your computer while operating through the Fortress Secure Client and unadvertised SSID. This was handled on each machine that was issued by the COASTS program prior to deployments and was briefed at various COASTS only meetings. *Validation* was the process of confirming that certain security measures were in place on your computer. This was verified by the Fortress ES-520 Access Point through the use of the Fortress Secure client. Optionally, the SutiSoft Secured BioNet was available to personnel with improper system capabilities to run the Fortress Secure Client.

Upon successful authentication and verification on the network, the Intrusion Detection System (IDS) was operated on all internal and external links and was the only rack mounted equipment on the network. Fortinet's FortiGate-500A Multi-Threat Security system provided high performance, flexibility, and security necessary to protect the tactical, mobile network. The FortiGate-500A platform featured two 10/100/1000 Ethernet ports which provided flexibility for networks running at gigabit speeds, 4 user-definable 10/100 ports for redundant WAN links (utilized with the IEEE 802.16 back haul links), high availability, and an internal 4-port switch for direct connectivity with the FortiGate-500A. Additionally, the FortiAnalyzer-800 provided storage and performance to log traffic and network congestion. Built-in log analysis provided a central point for consistent analysis of network utilization, Web activity, Virus activity, Spam activity, and Intrusion attack activity across multiple networks.

a. Biometric Device - SutiSoft Secured BioNet (SBN) Fingerprint Scanner

The SutiSoft equipment was tested on the network to verify that authorized users were accessing the TOC AP. The SutiSoft Secured BioNet (SBN) is a DSP-based device with its own processor, storage and RAM that provides fingerprint-based user identification access control of the enterprise network at the WiFi Local Area Networks (LANs) access point. The SBN was used in the COASTS-07 scenario to provide an additional layer of wireless access control to the TOC AP. The goal was to

deny network intrusions and the compromising of data over the wireless network regardless of packet sniffing techniques. By combining the latest Wi-Fi security (WPA2) and Biometric identity verification technologies, the Bio-NetGuard provided a highly secured access control mechanism for the COASTS-07 network. The diagram in the figure below shows the SBN server setup at the Wi-Fi Access Point during FTX V at Mae Ngat Dam, Thailand.

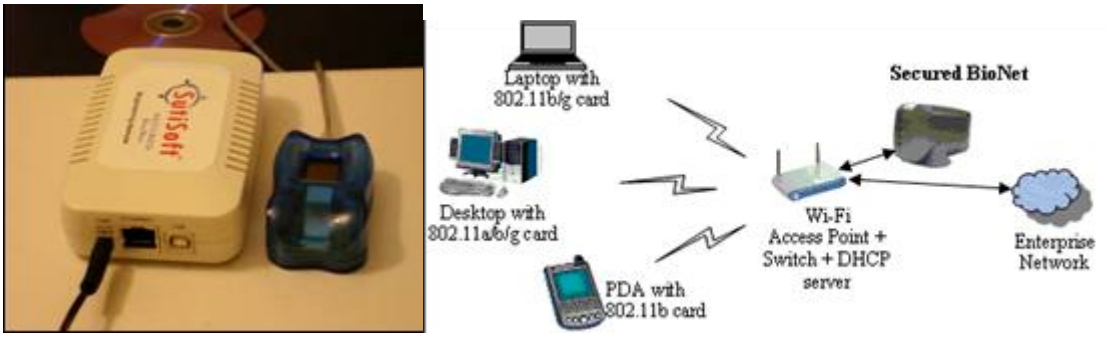


Figure 17. Secured BioNet (SBN - SutiSoft) Server & Finger Print Device. (From SutiSoft User Manual)

b. Biometric Device – DynaSig Bio Pen

The DynaSig Bio-Pen was used as an authenticator which, if passed successfully, allowed the user to gain access to the Fortress secure client. The DynaSig Bio-Pen was an access control method and verification tool for use in the field experiments. The Bio-Pen had the following advantages when compared to other biometric identification options:

- It had multi-factor authentication and used both behavioral and physical characteristics as determining biometric identifiers.
- It was a simple pen model, well accepted and easily implemented in the program and required no learning curve or "social" engineering.
- It was not intercepted or circumvented the way fingerprints or other physical biometrics devices have been.
- The Bio-Pen also acted as a physical "token," during shipboard operations, which not only generated a unique password at each signature verifying authority,

presence and cooperation, but also has the additional security option of allowing the further uniqueness that the signature has been made by a signer's assigned pen.

Figure 18. Bio Pen Enterprise Edition. (From DynaSig Bio-Pen User Manual)

c. Biometric Device – Identix RDT4

During shipboard operations the IBIS handheld biometric system, a subject's photo and forensic quality fingerprints (configured for two index fingers for this year) were captured on the IBIS handheld device. The fingerprint data was packaged into a National Institute of Standards and Technology (NIST) standard record and could be sent to the IBIS server via either access point, Cisco or Fortress, utilized on the MIO. (This portion was not done due to Biometric Fusion Center incompatibilities with experimental networks.)

When fully operational, the IBIS server submits the transactions to one or more designated Automated Fingerprint Identification System (AFIS) and other databases for matching, including, but not limited to: Identix ABIS System, third-party AFIS, warrant files, mug shot systems and demographic files. The IBIS server processes the match results. If a match occurs, the IBIS server retrieves demographics and other information from designated databases, and forwards the identity information – name and date of birth – back to the IBIS handheld device wirelessly. A summarized history, recent mug shot or photo, warrant or watch-list information, and other defined file histories can also be retrieved. If there is no match, the IBIS server wirelessly transmits the "NO

IDENT" result to the IBIS handheld. The fingerprint and photo are deleted from the system. During this experimental phase, all the data was collected in real time and transmitted to the Tactical Operations Center and verified against a local database to confirm or deny positive matches or to provide an updated situation report.

4. PORTABLE COMPUTING DEVICES

a. OQO Wearable Computing Device

The OQO was selected for its form factor, capabilities and ruggedness. The OQO model 02 computer with embedded HSDPA44 capability features unprecedented mobility at 142mm x 84mm x 25mm in size, less than 1 pound, and with ergonomic backlit keyboard and TouchScrollers; flexibility with a full docking station and support for dual external displays at up to 1920 x 1200 pixels through digital (HDMI/DVI) and analog (VGA) video interfaces; and power with up to 1.5GHz CPU, 1GB of DDR2 SDRAM, shock-mounted 60GB HDD with active drop detection, and compatibility with standard PC-based applications.

[44] High-Speed Downlink Packet Access (HSDPA) is a 3G mobile telephony protocol, which provides a roadmap for UMTS-based networks to increase their data transfer speeds and capacity. Current HSDPA deployments now support up to 14.4 Mbit/s in downlink.

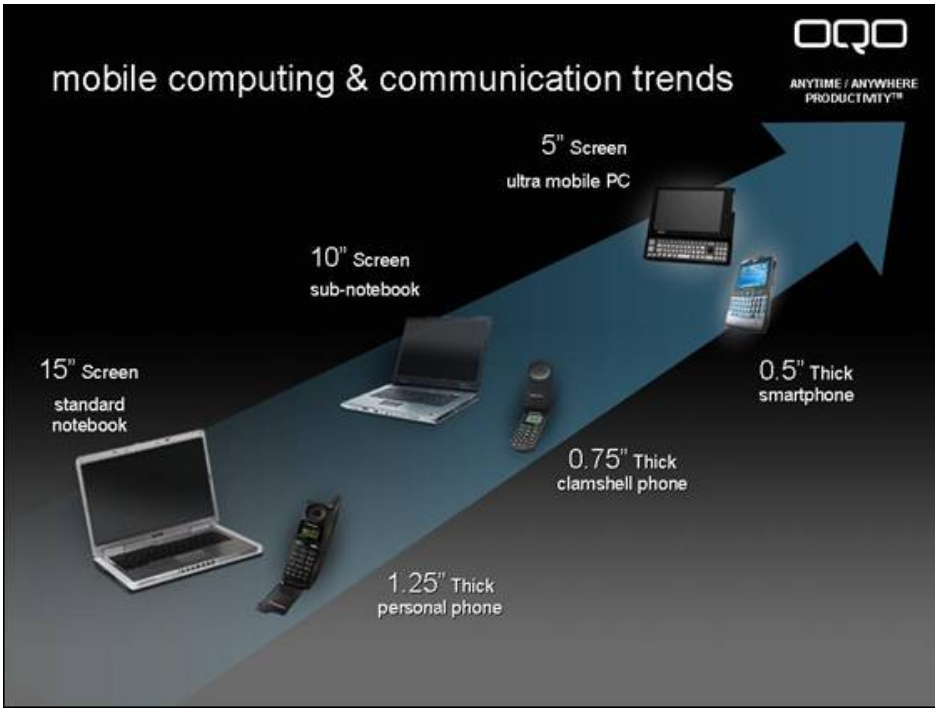


Figure 19. Historical perspective from laptop/cell phone to UMPC/Smartphone. (From www.oqo.com)

Figure 20. OQO Model 01 (Top) and Model 02 (Bottom).

The OQO has been used in a variety of exercises to include: MIOs, Humanitarian assistance operations, Search and Rescue operations, Video surveillance missions and networking configurations. Additionally, the OQO had a full Microsoft Operating System and was configured to operate video servers, mapping software (Falcon view), APRS, Radio over IP (Wave software) and Bio Pen simultaneously. Its IEEE 802.11 Atheros card allowed for authentication via the Fortress Secure Client through multiple Access Point configurations.

5. INTERNET PROTOCOL (IP) VIDEO EQUIPMENT

a. XVD

This XVD was selected as a pre-packaged device with the Grizzly and performed exceptionally well when handling various digital feeds. The XVD was an entirely new compression technology known for its high quality and high compressibility exceeding MPEG's. XVD could reduce data size to a fraction of a corresponding MPEG-2 file while maintaining its image quality. During COASTS-07, the XVD SD-TX100 was used as an ultra-compact, integrated video and audio encoder utilizing the IP network interface in conjunction with the Grizzly and delivered high-resolution, real-time digital content at low encoded data rates across the mobile IP network. Utilizing next generation XVD technology, the SD-TX100 provided the highest quality and resolution in digital video content at any given bandwidth, and delivered video at full D1 resolution[45] within IEEE 802.11a backhaul links. The SD-TX100 captured and compressed analog video and audio content (NTSC and PAL) into a high-resolution XVD data stream during unmanned aerial vehicle (UAV) flight and transmitted the signal to the iCOP through the mobile routers. Like the Grizzly's Mango DSP, the SD-TX100 encoder contained a compact DSP powered mini-server that connected directly to any analog TV source or IP-based network. Its mini-server mode enabled the SD-TX100 to transmit the compressed audio and video stream to multiple destination decoders[46] using a variety of transmission options.

[45] 525/30 or 625/50 lines/frames per second.

[46] SD-RX100 is the receiver for this transmitter and operate as a set.

Figure 21. XVD CamCast for Multicasting operations.

b. AXIS-213 Cameras

The AXIS 213 cameras were chosen for video surveillance due to their feedback from previous COASTS exercises. The AXIS 213 Pan Tilt Zoom (PTZ) Network Camera enabled remote monitoring with pan, tilt and zoom through the operator's control; from any PC connected to the LAN, WLAN, Internet or iCOP. It provided wide coverage with its ability to pan 340 degrees, tilt 100 degrees and zoom in on specific details as each authorized users requested. The AXIS 213 PTZ could be manually controlled for switching between color image during daytime, and black/white image in low light or nighttime conditions using the built-in IR lighting or the external IR lamp for longer distances. The AXIS 213 PTZ delivered Motion JPEG and MPEG-4 video streams simultaneously. It was ideal for monitoring inbound/outbound routes, security, MIOs and area activity.

Figure 22. Axis 213 IP Camera with PTZ. (From www.axis.com)

c. Integrated Common Operational Picture (iCOP)

The iCOP was chosen to bring the network into a TOC and was used as the focal point for all sensor devices. iCOP was a metadata-based system which provided a single visualization environment with capabilities appropriate to event, or user-specific requirements and was located in the TOC for command situational awareness and briefing. iCOP offered multi-mission capable C2 suites that allowed systems and users to interface with Global Information Network Architecture (GINA) through a spectrum of connected devices. The iCOP represented a revolutionary approach to information management and analysis through the correlation and aggregation of disparate sensors on the network. It is a new technology that does not yet exist in either the commercial marketplace or the DoD.

Figure 23. Integrated Common Operational Picture (iCOP) Display. (From COASTS)

D. SUMMARY

The Maritime Fly Away Kit – Gen II (MFLAKII) has been designed, tested and deployed for various field events, as well as, military exercises. The success of the MFLAKII hinges on its compact form, mobile capabilities and scalability. The form factor is small enough to deploy on a vehicle or small boat and produces a tactical footprint that supports the lowest echelon war fighter while providing near real time data, voice and video to the command echelons most in need of this information.

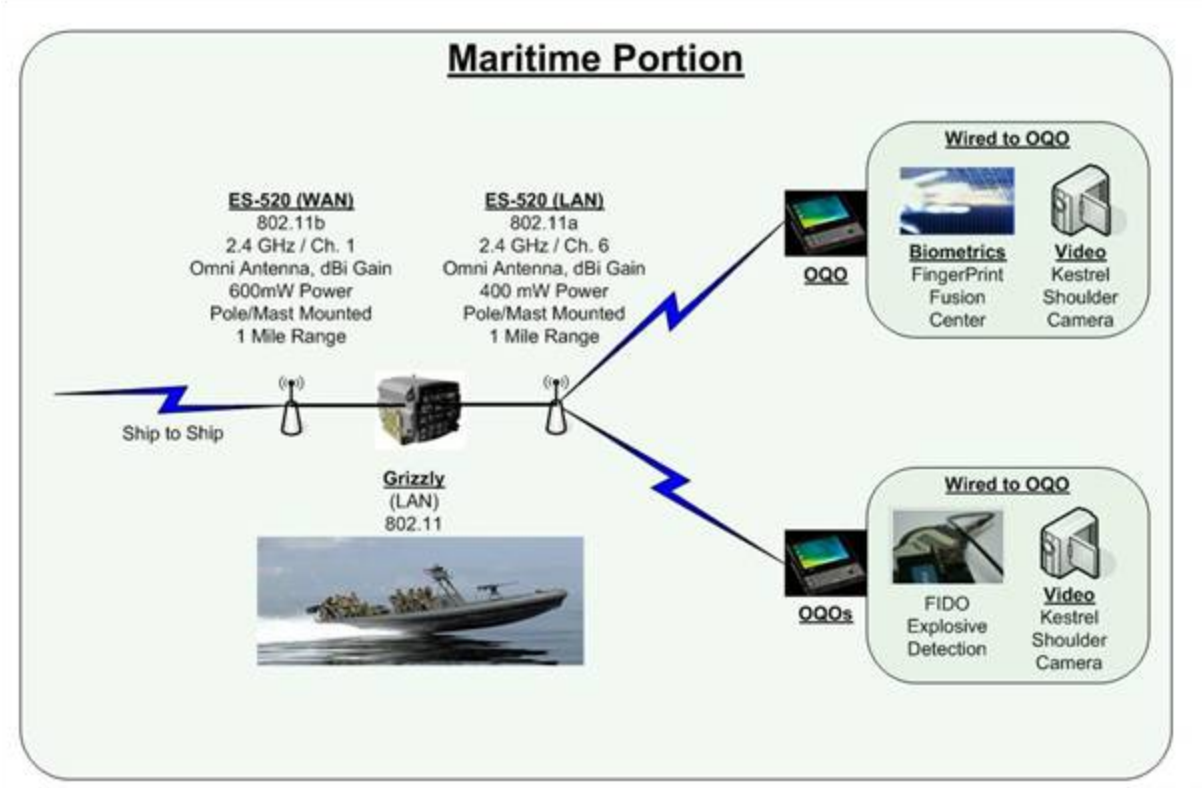


Figure 24. Maritime Fly Away Kit – Gen II (MFLAKII) as configured for SEACAT 2007.

As configured above, the MFLAKII used all technology components listed in this chapter. The seven meter RHIB platform contained one 1620 pelican case and held all the components necessary to conduct the operation. Other than the pelican case, a 10 foot carbon fiber mast was attached to the bridge of the RHIB for long haul communications. Since this is a scalable network system that relies on the TCP/IP protocol, it offers seamless roaming across multiple networks and creates an environment that revolves around net centric warfare. By employing the mobile routers in this system, MFLAKII was capable of transitioning from garrison to deployed networks without impacting either operational area. Mobility, scalability, compactness and form factor have combined to present a system that bridges the gap between stationary and mobile systems.

IV. SELECTION OF METRICS AND EXPERIMENT DESIGN

The COASTS-07 platform was designed around testing new and emerging technologies from COTS inventory. This year, COASTS-07 had several new technology vendors related to backhaul testing. The Motorola PTP 600, Redline's Family of AN30/50/80/100 radios, Fortress Technologies' ES-520 and Western DataCom / Cisco's 1Watt WMIC for embedded wireless access / bridging. This thesis specifically covered the AN-80i, ES-520 and WMIC components. Testing for the AN-50's was conducted in previous years and testing for the Motorola PTP600 series will be published in a separate thesis by another author.

Field Training Exercise I (FTXI), conducted in October 2006, was used as an orientation for future network testing as part of the COASTS-07 team exercises. Camp Roberts, California was the site of the first exercise and is located at the CIRPAS facility aboard Camp Roberts in California. The left side of the below figure showed NPS on the Monterey Peninsula and the right side depicted an aerial view of the CIRPAS facility. All components were available for data collection and training and are discussed in greater detail in Chapter III. No actual testing was done on the equipment

Field Training Exercise II (FTXII), conducted in January 2007, was used as a site survey evolution and network preparation exercise to support field requirements for COASTS-07. Fort Hunter-Liggett, California was the site of the second and third exercise and took place at the unimproved runway and transiting location. This location allowed for real world testing and provided realistic link scenarios to perform the required tests. The figure below depicts the site survey drawing prior to network setup.

Figure 25. Fort Hunter-Liggett Army Base in California. (From GoogleEarth)

Field Training Exercise III (FTXIII), conducted in February 2007, was used as the actual testing evolution and was manifested from FEXII. Since this exercise was also conducted at Fort Hunter-Liggett, it built upon the network configurations tested at FEXII and provided basic setup and configuration templates for the equipment. The unimproved runway was measured at 1.3 miles and provided a flat surface with which to conduct the tests. Weather data was collected for all testing days, but does not impact the test results. The following diagram shows the testing variables that were utilized.

The separate ground tests were used on the runway, in controlled environments, with similar heat indexes. Scenario One tested Redline's AN-80i, scenario two tested the ComCase's WiFi antennas and scenario three tested the Fortress ES-520.

Field Exercise IV and V(FEX IV and V), conducted in March and May 2007, respectively, were based at Mae Ngat Dam in Thailand which is located approximately 35 miles North of Chiang Mai. The training and testing at Camp Roberts and Fort Hunter-Liggett were used as training grounds for the deployment to Thailand. All successful implementations at the FTX's would be taken to Mae Ngat Dam for operational testing and further development. The below photo shows Mae Ngat Dam with water, vegetation and elevation changes. FEX IV and V would be used to tie together network tests conducted on the Monterey Bay (over water), at Camp Roberts (elevation changes) and Fort Hunter-Liggett (temperature variations).

Figure 26. Mae Ngat Dam in Thailand. (From GoogleEarth)

A. SCOPE OF THE TEST

The intent of the MFLAKII test was to demonstrate the use of the network mobile router with respect to various back haul solutions.

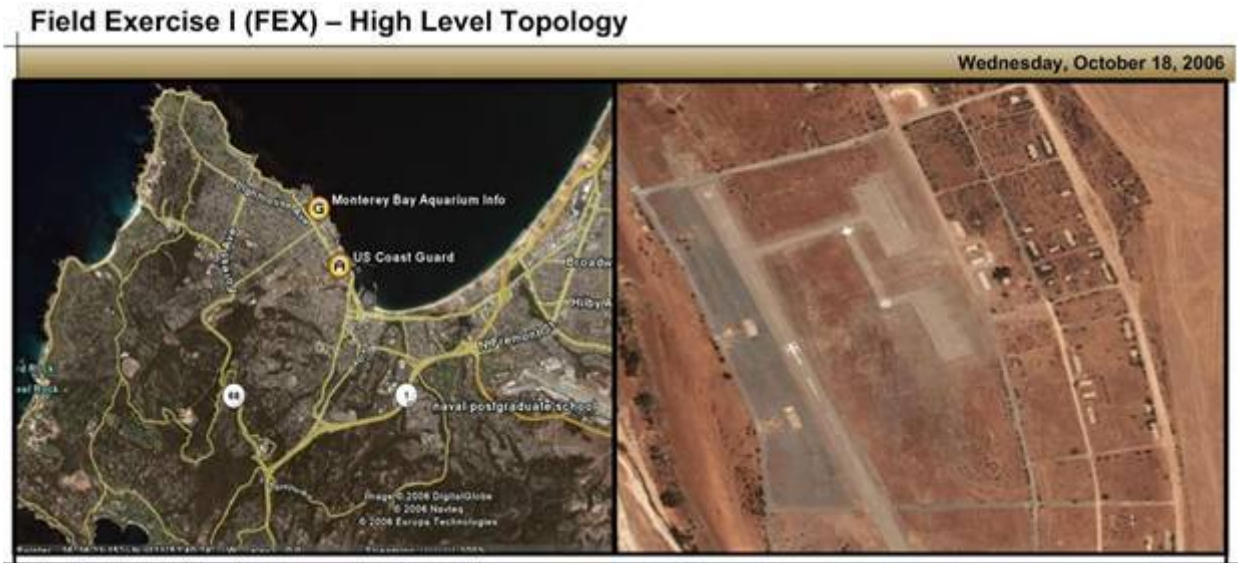

Field Exercise I (FEX) – High Level Topology
Wednesday, October 18, 2006
Monterey Bay Aquarium Info
US Coast Guard
naval postgraduate school

Figure 27. High Level Topology for Camp Roberts, California. (From GoogleEarth)

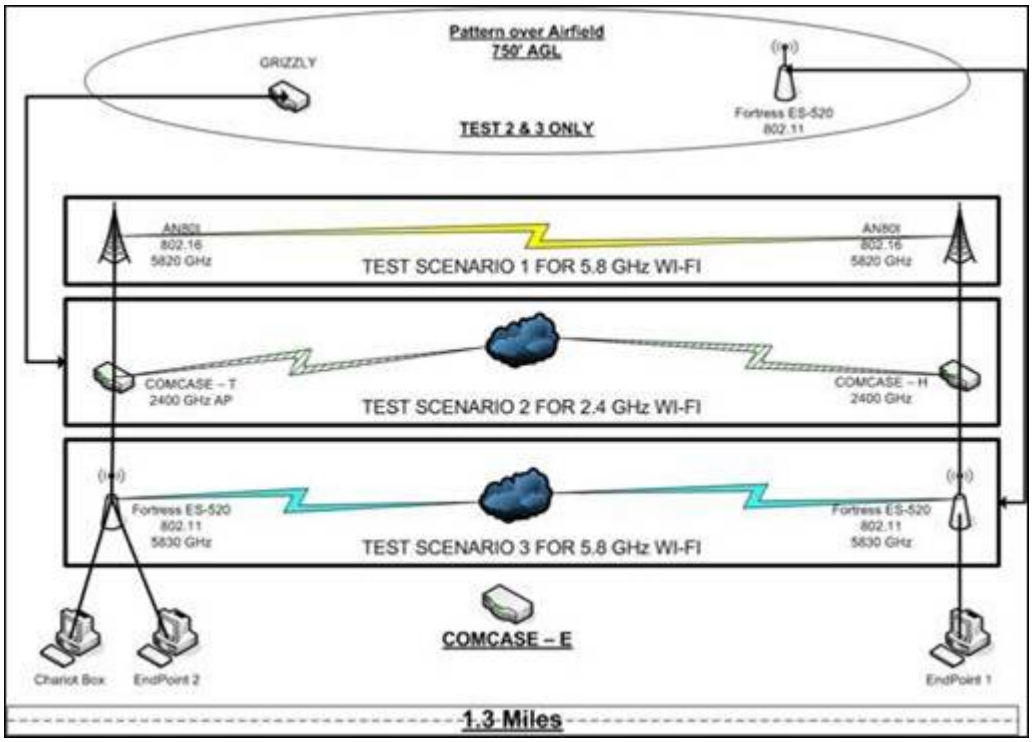


Figure 28. Network Diagram for Field Exercise II, Fort Hunter Liggett, California.

The tests at Fort Hunter Liggett started at the southern end of the runway as designated by Endpoint #2 in the figure above. Scenarios 1, 2 and 3 are used individually to test throughput, response time and video streaming across the airfield. The airfield is

1.3 miles long and the northern end of the runway is configured with another laptop labeled 'Endpoint 1'. All tests were conducted through the ComCase which utilizes the Cisco 3200 Mobile Access Routing platform and it was located between 'Endpoint 2' and the respective back haul link for that test. The tests were conducted through the ComCase since there was a requirement for the TOC router to be implemented in the total network solution.

The first test utilized the Redline AN-80i IEEE 802.16 radio transmitter at a frequency of 5820 MHz. Channel spacing was set at 20 MHz, antenna gain was 16dBi (directional), the master transmitter was at the southern end and no encryption was used.

The second test utilized the Cisco 1Watt WMIC radio transmitter at a frequency of 2400 MHz. Channel 11 was used for deconfliction reasons, antenna gain was 12dBi (directional) and no encryption was used.

The third test utilized the Fortress ES-520 radio transmitter at a frequency of 5830 MHz. Channel spacing was set at 20 MHz, antenna gain was 16dBi (directional), the root transmitter was at the southern end and no encryption was used.

Additional testing was done using a Cessna aircraft flying at 750 feet above ground level (AGL). This testing used the ComCase T and Grizzly mobile routers while utilizing the Cisco 1Watt WMIC radio transmitter. The test used a 120 degree sector panel with 16 dBi gain. The antenna was also retrofitted with a metal back plate to eliminate or reduce back and side lobe losses. Although testing data was not collected, video was streamed through the mobile routers from a base altitude of 750 feet to 5,000 feet while the Cessna circled the airfield. Video was captured through the Grizzly's DSP Mango card and viewed on the ground in real time.

B. SELECTED METRICS

The selected metrics for this series of tests were in accordance with the COASTS-07 Field Exercises and Deployment schedule. The tests demonstrated the networks' capability to handle multiple video streams across the network. Additionally, it helped determine the correct back haul components necessary to support video streaming operations. Lastly, the tests helped scope COASTS-08 the selection of the proper

protocols necessary to further enhance video streaming in the future. There were multiple protocols available to demonstrate video streaming (e.g. TCP/IP, UDP, RTSP, Unicast, Multicast and P2P) but only TCP/IP was tested since it is directly attributed to the MFLAKII through the mobile IP scheme. The metrics used for this test were: *throughput* as measured by bulk transport capacity, *response time* as measured by roundtrip delay and loss and *video streaming* as measured by throughput thresholds on video packets.

Throughput measured the maximum data throughput rate of a communications link or network access. The standard method of performing a measurement is to transfer a 'large' file and measure the time taken to do so. The throughput was then calculated by dividing the file size by the time to get the throughput in megabits, kilobits, or bits per second.

The Response Time was a measure of effectiveness related to the amount of time it took a data packet to traverse the distance. Stated differently, it was the elapsed time between the end of an inquiry on a computer system and the beginning of a response. Network performance monitoring tools were configured to measure and display various parameters characterizing communications between or among a pair of network endpoints. In TCP/IP-based networks, one such parameter was the network Round Trip Time (RTT). Figure 25 mandated that both network endpoints (i.e., both the client computer Endpoint 1 and the other computer Endpoint 2) were instrumented with IxChariot Endpoint software in order to monitor the various times. As a control measure, the RTT was measured from the 'Chariot Box' location on the southern end of the runway. This eliminated any inconsistencies related to tests taken at various locations.

Video streaming referred to the ability of an application to play synchronized media streams like audio and video streams in a continuous way while those streams are being transmitted to the client over a data network.

C. MEASURES OF EFFECTIVENESS AND PERFORMANCE

The COASTS-07 exercises provided an environment in which to test the qualitative measurements of the MFLAKII. The Measures of Performance (MOP)

directed that the bandwidth performance and throughput for a network were the most important factors for testing. As stated earlier, the AN-80i, ES-520 and WMIC were tested on these parameters. The qualitative measures were taken from the COASTS-06 AAR that showed considerable network degradation during high bandwidth usage and video streaming evolutions. Several other non-network items were tested during COASTS-07 but qualitative data was unnecessary during these evolutions.

For the Measures of Effectiveness (MOE), RF Monitor and IX Chariot were used to collect the pertinent information related to data throughput and bandwidth performance. This data was collected and downloaded into a .csv file

1. Test Equipment

There were three laptops used in this demonstration. Those laptops include one Sony Vaio (EndPoint1), one Dell Latitude D600 (Chariot Box) and one Dell Latitude D600 (EndPoint2). All laptops' CPUs are at least Pentium IV, 1.5GHz processor with memory of at least 256MB, which provided enough capability to support the network performance test. This eliminated the concern about laptop processing conflicts while running the network tests. All other components, to include the wireless cards, were disabled so as not to affect the outcome of the tests.

All laptops were configured with Windows XP Service Pack 2 and IxChariot Endpoint software to collect the signals for the IxChariot software. All other software packages were stopped during the operation of the tests.

The ComCase and all associated radio components were outlined and discussed in Chapter III.

2. Testing Equipment

IxChariot was used as the basic network software package to conduct all tests. IxChariot is a test tool for simulating real-world applications to predict device and system performance under realistic load conditions. Comprised of the IxChariot Console, Performance Endpoints and IxProfile, the IxChariot product offers thorough network performance assessment and device testing by simulating hundreds of protocols across

thousands of network endpoints. The IXChariot license was obtained through the Naval Postgraduate School and was used to capture all data points from the various technologies.

The MS2711B Anritsu Handheld Spectrum Analyzer, covering the 100 kHz to 30.0 GHz frequency band, was used to verify radio frequency outputs for all tested radio systems. This was done in conjunction with COASTS-07 Field Exercise III with the Joint Electronic Warfare Center (JEWC).

D. TESTING

The first test was used to capture the Response Time of the network device at Layer 2 (Transmission) of the OSI model. The Response Time is a key variable in establishing the baseline response for each component. In the first test (see Figure below) the Response time for Fortress (#1), AN80I (#2) COMCASE H (#3) and COMCASE T (#2) was captured. In this case, the 1.3 mile link between Endpoint #1 and Endpoint #2 was measured in fractions of a second (It is the vertical scale, even though it is not labeled correctly). Side note: this was a closed network as depicted in the topology diagram, and did not have anything else that contributed to the response time. All components on the topology remained in place during all instances of the test. There were no variations or configurations changed during the tests on any platforms.

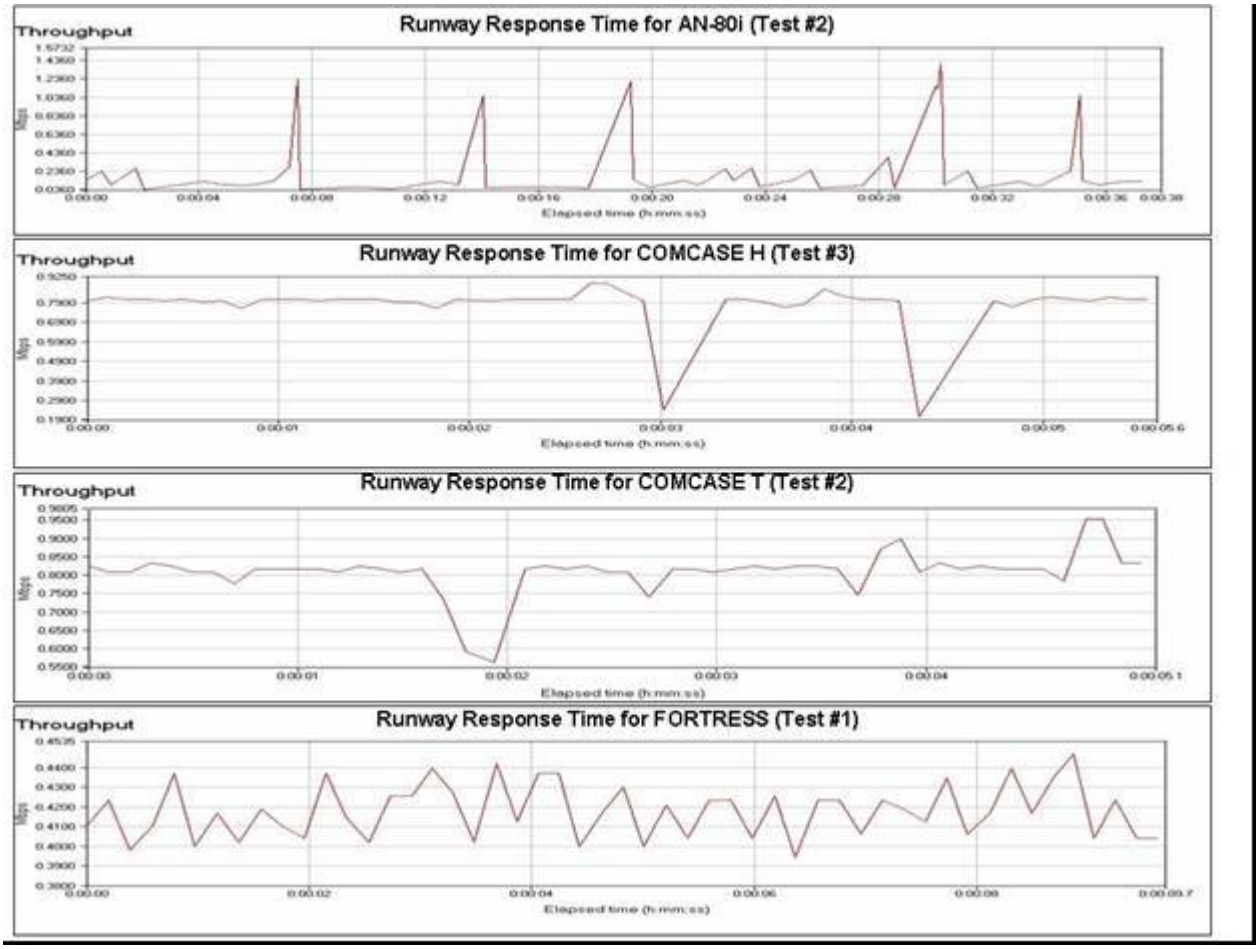


Figure 29. Response Time for Test 1, 2 and 3 on Back Haul Radio Transmitters.

This series of tests (Figure 21) showed the Response Times for each respective radio system. The Fortress ES-520 demonstrated an average response time of .42 milliseconds and proved to be the system with the lowest and most stable response time overall. The Redline AN-80i demonstrated excellent response times, average of 1.9 milliseconds, but also showed an increase or spike during the tests. This spike in activity was unexplained and led to an inconsistent response time across the network. Consequently, this test was run six times during the two-day process and revealed the same tendencies each time. The ComCases were very stable with response times averaging approximately 0.8 milliseconds for each. The Response Time clearly favored the ES-520, but does not conclusively decide a superior product, but established an important baseline measurement for future aggregated measurements.

The second test captured Throughput data, which is the amount of data transmitted through the connectors in response to a given request. This portion of the test covered Throughput testing for the AN80I (#2), ComCase H (#1), ComCase T (#2) and Fortress (#1). All devices were operated in the 5.8 GHz frequency spectrum. The ComCase equipment was demonstrated through the AN-80i as opposed to the streaming of the Fortress ES-520. The AN-80i is based on the 54 Mbps version of firmware.

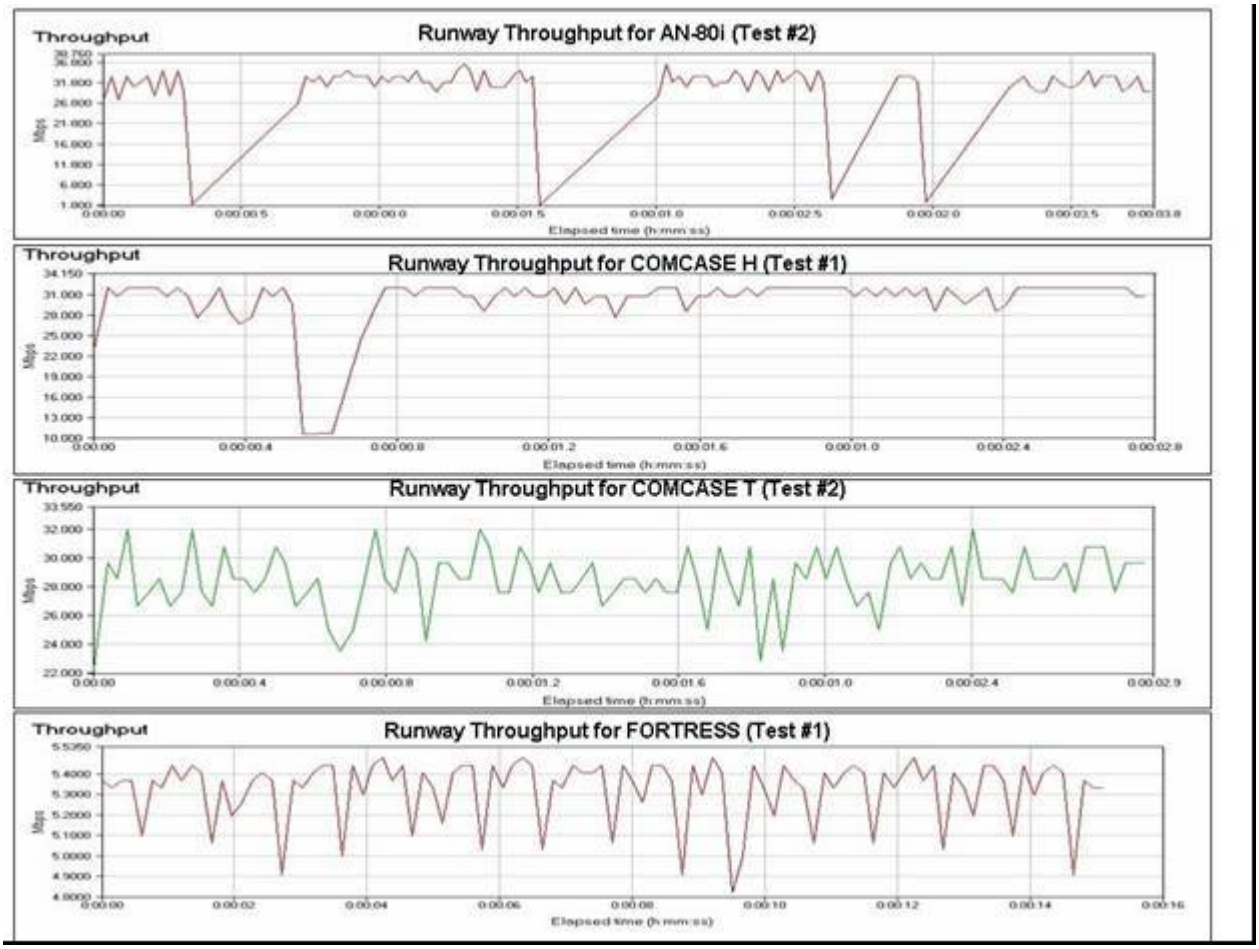


Figure 30. Throughput for Test 1, 2 and 3 on Back Haul Radio Transmitters**.**

The major difference was in the throughput level of the AN-80i at 32Mbps and the Fortress ES-520 at 5.3 Mbps. This throughput level was directly associated with the limitations of each respective standard. IEEE 802.11a used in the Fortress ES-520 performed as the specification states and the Redline An-80i showed similar throughputs

for the level of firmware associated with this equipment. This test has a conclusive outcome that supported the MoP and MoE by delivering a 6 fold increase over the throughput of the ES-520.

The third test captured throughput in terms of video streaming. Video streaming was measured against a minimum 300 kbps downstream which supported RTP/RTSP (This is described in Chapter III). It covered the ability of the platforms to stream video through the respective devices. All tests were run on the same day under ideal conditions. Runway Video Stream for ComCase H with AN-80i (#1), ComCase T with AN-80i (#1) and Fortress (#1) are listed below.

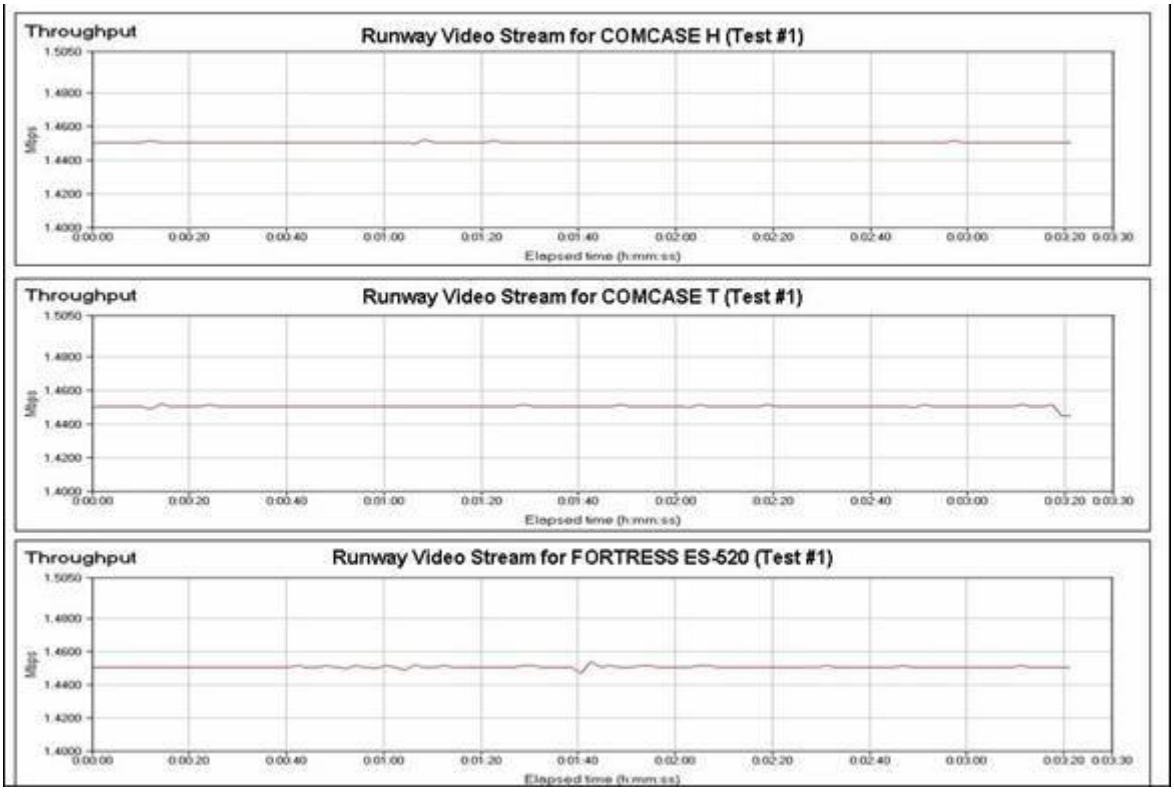


Figure 31. Video Streaming for Test 1, 2 and 3 on Back Haul Radio Transmitters.

Figure 28 showed that the AN-80i and the ES-520 were capable of delivering stable TCP/IP video streams across the network. The results indicated that all tested platforms streamed the video at 1.544 Mbps which led to the conclusion that multiple 300 kbps feeds could be handled by each device in a controlled environment.

Overall, the tests were successful and proved that the Redline AN-80i exceeded the transmission intervals and video streaming capabilities of the Fortress ES-520. As a trunk line, the AN-80i provided solid, video streams from multiple sources, whereas, the Fortress ES-520 was not capable of handling more than 4 video streams at one time (4 streams * 300kbps = 1.2 Mbps). This may be addressed in the future with the selection of different protocols or the transition to a network fully dependent on IEEE 802.16 technologies.

E. GENERAL OBSERVATIONS

The selected tests were used as part of the design and implementation process prior to selecting a network to take to Thailand and follow-on exercises. They should be a basis for determining future uses of network components and future acquisitions or partnerships related to COASTS-08 projects. There were tests completed in a variety of states: ground-to-air, ground-to-sea and ground-to-ground. These simulations represent the scenarios closely related to MDA concepts and support continued research into NCW concepts. Although data was not collected in all environments, there are significant advances for backhaul communications related to ground-to-sea testing and sea-to-sea testing that are prime for data collection. With the number of successful trials at sea, the next test should capture these measures of effectiveness during different sea states and other varieties of ship-to-ship and ship-to-shore engagements.

In working with air assets during the Fort Hunter Liggett demonstration, it was demonstrated that IEEE 802.11g was capable of providing streaming video. This capability was demonstrated with the Grizzly which demonstrated mobile IP concepts as well as video streaming. Additionally, the Grizzly utilized its ‘at care of’ address in order to network to the TOC router during the air scenario. The use of mobile IP and streaming video directly relates to MIO exercises where helicopter assets are included and kept abreast of situations on a boarded vessel. Additional areas of research show great promise in the United States Coast Guard where a variety of ships and air assets are called upon to engage various vessels and other related situations.

Another observation is related to weather. During various scenarios, the equipment deployed to many remote regions. This uncovered two additional problems that required great attention and resources: temperature and wind. The temperature extremes for the equipment varied from the hot and humid conditions of Thailand and the freezing conditions experienced in Fort Hunter Liggett, California, near the tops of the mountain ranges. There seemed to be some discrepancies in operating temperatures of equipment and actual operating thresholds cited in technical manuals. Specifically, some of the equipment would perform well in the hot, humid environments through the use of heat sinks and thermal plates for dissipation and others would perform well in regards to cold and rain. Although most of the equipment performed well, these limitations should be documented for future use and planned for when in that environment.

This chapter introduced and discussed the equipment used to test, the process of testing and the evaluation of the systems. The attributes of an effective metric, measures of effectiveness, and measures of performance were introduced. The metrics, MoP and MoE used to evaluate the integrated network performance was vital. The specific tests and processes were described in detail. Finally, this chapter concluded by describing general performance characteristics that will be used to help develop, plan, and test an integrated network for future COASTS exercises.

THIS PAGE INTENTIONALLY LEFT BLANK

V. MARITIME FLY AWAY KIT GENERATION II

A. COMPOSITION

The MFLAK-II was designed and built for deployments and operational areas that require the use of mobile, rugged and lightweight communications suites capable of sustained operations in adverse weather conditions and environmental conditions. The MFLAK-II was deployed in various configurations based on operational need and capabilities of the on-scene commander. Predominantly, the suite traveled in three sections: Garrison, Mobile and Mission Enhanced components.

1. Garrison Components

The Garrison components were associated with the TOC or NOC and pertained to restricted operating environments. As mentioned in Chapter III, the ComCase T is the main centerpiece of the Garrison components. In order to efficiently address the requirements associated with COASTS-07 and Royal Thai Air Force requests, the following software packages were installed: Wide Area Voice Environment (WAVE), What's Up Gold, Cisco Call Manager, Solar Winds Orion-Enterprise Edition and RF Monitor. WAVE was used for voice communications between the TOC and mobile node. WAVE software was used on the IP network to build an infrastructure that was used for formal and informal communications between groups of participants. It was also integrated in the Call Manager Express for connecting mobile users to VOIP users in the TOC. What's Up Gold handled network monitoring which utilized a windows-based application that documented trends and assisted with resource planning. Solar Winds Orion-Enterprise Edition was used for SNMP queries of the radio links and assisted with troubleshooting during initial setup and follow-on operations.

2. Mobile Components

The Mobile components were generally associated with austere operating environments that ranged from remote operations areas supporting UAV operations to vehicle engagements to aircraft platforms.

Figure 32. MFLAK Grizzly mounted on CDR Schmidt's Cessna.

In Figure 32, a Cessna aircraft was used to demonstrate the mobile nodes capability to stream video from the aircraft through the Grizzly and into the TOC where the receiving garrison ComCase T was located. The Cessna was able to maintain communications, with constant streaming video, at altitudes greater than 5,000 feet AGL and ranges to ¾ -1 mile depending on altitude. Degradation was noted in the communications link during steep banking turns or landing scenarios, but links were reacquired when movements were completed. Additional scenarios utilizing roving vehicles demonstrated wireless handoff scenarios where video streams, voice streams and data transmission were done through multiple moving engagements. These simulations helped understand the fluid environments associated with ship-to-ship environments dealing with interrogator vessels approaching unknown vessels.

The Grizzly (Figure 33) at the UAV site was used as a relay between several aircraft types. The AeroVironment Raven and the CyberDefense CyberBug used the Grizzly to receive digital signals through the radio control links and transmitted them to the TOC through long haul radio links. This technology was used in conjunction with

Multicasting protocols to allow the TOC, Thailand and US (stateside) counterparts to observe the video from the UAV's in a near-real time fashion. This capability was a tremendous asset for viewing in the TOC and issuing follow on orders to the UAV pilots.

Figure 33. Grizzly faceplates configured with IVS at UAV Site.

3. Mission Enhanced Components

Some of the components adapted for use through the COASTS experiments and implementation come from new products, COTS and GOTS. For use in the maritime portion and in conjunction with SOF personnel, Falcon View software has been utilized on the OQO's. Falcon View is a mapping system that displays various types of maps and geographically referenced overlays. The scenarios used satellite and elevation overlays to gather GPS data which was overlaid on the mission planning documents. Falcon View also supports a large number of overlay types that can be displayed over any map background and transferred to a wrist display for easier operation. Figure 31 shows the mapping display as used at Fort Hunter Liggett in February 2007.

Figure 34. Wrist mounted mapping device with USB connection.

Another mission enhancement was the use of the JABRA Bluetooth head pieces. The JABRA earpiece was used in connection with the OQO and the WAVE software for voice communications to the TOC. This allowed for hands-free, voice operated communications while conducting tasking and scenario engagements. Voice communications through the JABRA earpiece connected through the Bluetooth receiver on the OQO and the OQO was wirelessly connected to the Grizzly. This configuration allowed for voice communications throughout the WAN while utilizing mobile networks components.

Figure 35. Boarding Party components for two personnel.

Additional functionality was added through the use of a shoulder mounted camera. The Kestrel Camera functioned through the USB 2.0 port on the OQO and acted as a video server in conjunction with the Smart Eye software installed on the OQO. The Kestrel was attached to several harness assemblies and the flexible leg stands allowed for greater functionality in mounting to boats and vehicles.

B. STANDARD OPERATING PROCEDURES (SOP)

1. Preparation of Equipment

During the COASTS-07, the team deployed eight times for full mission support and multiple times for testing and development. The preparation necessary for a field deployment includes: vendor coordination/support, logistics of necessary equipment, coordination with supporting agencies, team training, set-up, preventative maintenance and pack-out requirements. Prior to departure the vendors were contacted for assistance in configuration, training, support and technical expertise. Logistics was done in conjunction with a local Logistics Officer who facilitated customs and travel necessities. The coordination from supporting agencies was completed through Naval Messages and telephone contact when appropriate. Additional coordination was done through email for international participants. Team training was completed prior to every deployment and supervised by the COASTS Student Lead and the Exercise Student Lead.

For the equipment preparation, each MFLAK required power through AC or DC means and incorporated inverters into the kits for efficiency. Pelican cases were used to transport the gear in their pre-formed structures and provide the necessary support and protection for the communications equipment. Pack-out kits were completed in conjunction with the Logistics Officer for compliance with airline standards and weight specifications.

The generation of documents for the Concept of Operations, Network Topology, billeting requests, test plans and timelines were completed and reviewed by the Program Manager prior to all operations. These documents provided the basic necessities for any field exercise, regardless of size.

During some of the exercises stateside, the NEMESIS[47] vehicle was utilized as a means to gain satellite connectivity. This satellite connectivity was essential and supported COASTS-07 in its field exercises in Fort Hunter Liggett and Camp Roberts, California.

2. Testing of Equipment

The testing of equipment was the major portion of this thesis and the exercises related to COASTS. As a test bed for experimental and trial components, the testing portion was the main emphasis. For testing, vendor participation was the key to success. Their technical savvy, know-how and time were the most crucial element in demonstrating the capabilities of their equipment. In particular, the ComCase and Grizzly components were laboratory tested for many hours prior to actual field implementation. This testing was used to configure the routers to operate with functions such as: OSPF, Multicasting, Virtual Private Networking (VPN), Voice Over IP (VOIP), Bridging Access Points, DHCP, Encryption and Mobile routing configurations. All configurations are listed in the Appendices for reference and provided the basis for configurations in all COASTS-07 exercises.

Additional testing was done to support radio links for AP's and back-haul links. These radio links were tested prior to the experiments and documented in the network topology for use by all personnel. The links were tested through RF Monitor and Solar Winds Orion for improved signal strength and decreased Signal to Noise ratios.

Peripheral testing was completed by vendor specifically supporting their product and used in the field experiments to test functionality, networkability and usability while supporting the various scenarios associated with COASTS-07.

3. Operation of Equipment

The equipment was operated in desert, sea and humid environments. Due to these conditions, the utmost care and time was taken to ensure the equipment was operated

[47] A mobile communications vehicle (Motor Home) retrofitted with routers, switches, satellites and computers for emergency scenarios.

safely and effectively. Additional measures were taken (i.e., weatherproofing, installing lightning protectors, grounding, etc.) to ensure the equipment was operated in a safe fashion. Since this equipment was designed for various scenarios and user engagements, the configurations were set so that the operators would have to mount the equipment and power it on. No further configurations were necessary after the testing phase. This allowed the operators to focus on actual exercises operations vice network configurations.

C. SUMMARY

Overall, the functionality of the Garrison, Mobile and Peripheral components was a vast improvement over past COASTS operations. The configurations of the network components will remain in place for COASTS-08 with little to no change in configuration of the base components. These packages were built with scalability in mind and COASTS-07 is currently purchasing additional ComCases to support larger scenarios which operate off of the same configurations in the appendices.

The peripheral devices tested were used in a Plug and Play manner and required little to no additional configuration (except video server for multicasting from the OQO). This allowed for quick adaptations for items like Falcon View, Bio-Pens and Kestrel devices.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION AND RECOMMENDATIONS

A. CONCLUSION

The MFLAK-II proved to be an outstanding generational improvement in terms of physical attributes, capabilities, ruggedness, operations and robustness. The MFLAK-II is currently used to support real world scenarios and has been used in air, land and sea environments. The original MFLAK thesis[48] identified several future research areas and questions and this thesis has addressed a number of those areas and has come up with additional research topics to better sustain and gauge the growth of this asset. The major areas of research and questions from the first generation MFLAK are as follows:

- Electronic Steerable Antennas
- IEEE 802.16 Amplifiers
- Satellite communications
- Riverine Communications Doctrine
- IEEE 802.16 Vendors for variability
- Multiboat PtMP IEEE 802.16 testing
- Alternate Network topologies
- M-FLAK CONOPS
- M-FLAK Periphery Technologies

As with most cutting edge technology, some of these areas have been addressed by the passing of time. Self-aligning OFDM antennas, IEEE 802.16 amplifiers and IEEE 802.16 vendors have been addressed and are evolving currently. The alternate technology with Fortress communications proved well-suited for a tactical environment and handled both LAN and WAN network topologies while encrypting the data exchanged. Additional peripheral items were explained in Chapter III.

[48] Robert Hochstedler, "Implementation of a Modular Fly Away Kits (FLAK) for C4ISR in Order to Counter Asymmetric Threats in the Coalition Riverine and Maritime Theatres." Naval Postgraduate School (NPS). Monterey, CA. June 2006.

1. Key Findings

a. Ruggedized Equipment that is Not Rack Mountable

The preponderance of equipment that is used for Hastily Formed Networks (HFN) or Fly Away Kits (FLAK) are rack mounted gear designed to function in a laboratory or secure environment. More often than not, this type of platform must be capable of quick deployment, open source access and scalability. This equipment must be in a small form factor capable of transiting within FAA regulated airlines and should not necessarily be a tightly secure network. Although security is handled through secure clients, username/password handling and MAC address filtering, the goal of the network is rapid deployment in austere environments.

b. Mobile Networks Exist to Support Operations

The ComCase suite of equipment is inline with mobile operations. The pursuit of PC/104 form factor components, heat dissipating equipment, power inverters for handling dirty power and components capable communicating while in a mobile environment are the basis of a mobile network. Additional mobile nodes can be added for scalability and robustness can be handled through the various protocols enabled on the routers and the implementation of QoS measures.

c. Technology is Not the Only Answer

Although this thesis is mainly about the technical solution behind MFLAK's, there must also exist doctrine, policy and TTP's that support this technology. Leaders must recognize the importance of this technology and leverage it in a way to support the first responders so that the gear becomes and asset and not a paper weight. Furthermore, the technology can be improved, but supporting technologies must also be improved. For example, there are a plethora of devices that can be implemented within an open source network, but each must conform to similar standards or the implementation will consume the operators, thus making this technology of little use.

d. Deployment Scenarios Must be Realistic

In setting up equipment, even MFLAK style, there must be time set aside to ensure the network is stable prior to adding in the components that support the first responders. The advanced party must be capable of implementing the design topology, commander's intent and socialization of the local personnel. The designed topology supports the mission and lays a framework to operate in the environments that MFLAK's excel in. Although the topology is used as a guideline, the changes must be documented and stored within a knowledge management structure so that the added components can be implemented in the future. Commander's intent must be used to guide the installation of the network. In chaotic, extreme conditions, the MFLAK must be capable of supporting and enhancing the Commander's intent while serving the needs of the operators and first responders. Lastly, the advanced personnel should be skilled enough to handle relationships that require clear communications. Communications is the key designing a network that supports Commander's intent and is within local regulations.

B. CONCLUDING REMARKS

1. Future Research

The components used to support the TOC and Mobile node operations were the basis for COASTS-07. There is a tremendous amount of additional research that can go into the network topology and interactions between networks and end user devices. For NCW, MIO and COASTS implementations, the following is a list of pertinent directions to research:

a. PC/104 Form Factor

The introduction of small form factored equipment is on the verge of engulfing all components. This includes radio, satellite and access point components. By decreasing the footprint of these devices and installing them into the ComCase, the scalability and robustness of the network increase and the logistical footprint decreases.

For exercise SEACAT-07, there were a total of (10) pelican cases sent to support a Maritime Interdiction scenario. The majority of the equipment sent would benefit from further research into PC/104 components and integration into the ComCase equipment.

b. Software Development

The preponderance of equipment being tested today focuses on the hardware components related to COTS equipment. There is little emphasis placed on software engineering or development which can enhance the current hardware capabilities. Unfortunately, this is a time consuming process and may not be suited for this type of environment. However, future interactions with software vendors and developers may produce greater returns when coupled with the advance hardware suites currently being tested.

The GPRS transmitter (hardware) and the software used to integrate GPRS feeds into WhirlWind shows the incredible capacity of a combined hardware/software solution.

Future ideas for software include: full WAVE implementation combined with VOIP components, Network Management software capable of managing mobile nodes, RF software used in conjunction with Anritsu components for greater Fresnel zone calculations and improved RF deconfliction.

c. Power Consumption and Distribution

In 2006 alone, U.S. datacenters consumed about 61 billion kilowatt-hours (kWh) of electricity or roughly 1.5 percent of all U.S. electricity consumption. That much energy cost about $4.5 billion, according to the report, prosaically titled "Report to Congress on Server and Datacenter Energy Efficiency." The power requirements of the equipment used to support operations carries a heavy burden. By definition, the MFLAK-II is used as a mobile fly away kit capable of sustaining data/voice communications for a particular area of need.

The trend of hardware developers that increases the energy costs is counter productive when dealing with MFLAK technologies. MFLAK technologies should focus on efficient power consumption, solar panel generators and other alternative power generators. In harsh environments, remote locations and emergency disaster areas, the majority do not supply their own power and rely upon supporting agencies to provide this power.

Future ideas should include the alternative energy sources that yield energy gains, vice energy hogs. Solar and wind energy show the most promise, but require complementary power systems to sustain or moderate flow during times of reduced power (i.e., no sun or no wind).

2. SUMMARY

Overall, the MFLAK-II benefited from the tremendous effort of COTS producers to make systems that support the military and first responder personnel looking for solutions that work in real environments. The MFLAK-II was successfully designed, tested, implemented and deployed during 2006-2007. This system supports NCW, MDA and the further progression of COASTS by supporting the long term need of the operator. The MFLAK-II is a lightweight, mobile, ruggedized communications suite with robust, scalable attributes that support high-end missions requiring data, voice, video and sensor recognition. The new MFLAK-II has many advances left to conquer, but is the best solution today to address the needs of future operational scenarios.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A –ROUTER CONFIGURATIONS

COMCASE T (CORE OF THE NETWORK)

```
hostname HAFA_CCT
boot-start-marker
boot-end-marker
enable password cisco
no aaa new-model
ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.100.81 192.168.100.85
ip dhcp excluded-address 192.168.100.65 192.168.100.70
ip dhcp excluded-address 192.168.200.1 192.168.200.10
ip dhcp pool local_Lan
  network 192.168.100.64 255.255.255.240
  default-router 192.168.100.65
  dns-server 203.146.237.237
  lease infinite
ip dhcp pool AP
  network 192.168.100.80 255.255.255.240
  default-router 192.168.100.81
  dns-server 203.146.237.237
  lease infinite
ip dhcp pool LAN
  network 192.168.150.0 255.255.255.0
  default-router 192.168.150.1
  dns-server 203.146.237.237
  lease infinite
no ip domain lookup
ip multicast-routing
multilink bundle-name authenticated
template Tunnel100
crypto isakmp policy 1
 encr aes 256
 authentication pre-share
 group 2
 lifetime 60
crypto isakmp policy 2
encr 3des
authentication pre-share
group 2
crypto isakmp key 1qaz@WSX3edc address 0.0.0.0 0.0.0.0
crypto isakmp nat keepalive 20
crypto isakmp client configuration address-pool local dynpool
crypto isakmp client configuration group HHDE01
```

```
key password
pool dynpool
crypto ipsec transform-set transform-1 esp-aes esp-sha-hmac
crypto ipsec transform-set NPS_VPN_Mesh esp-3des esp-md5-hmac
no crypto ipsec nat-transparency udp-encaps
!
crypto ipsec profile SDM_Profile1
 set transform-set NPS_VPN_Mesh
!
!
crypto dynamic-map dynmap 1
 set transform-set transform-1
crypto map dynmap isakmp authorization list HHDE01
crypto map dynmap client configuration address respond
crypto map dynmap 1 ipsec-isakmp dynamic dynmap
interface Loopback0
        ip address 192.168.100.1 255.255.255.240
        ip pim dense-mode
interface Loopback10
        ip address 10.10.10.10 255.255.255.255
        ip pim sparse-mode
interface Tunnel0
        bandwidth 1000
        ip address 10.10.100.1 255.255.255.0
        no ip redirects
 ip mtu 1300
 no ip next-hop-self eigrp 100
 ip nhrp authentication DMVPN_NW
 ip nhrp map 10.10.100.100 205.155.65.87
 ip nhrp map multicast 205.155.65.87
 ip nhrp network-id 100000
 ip nhrp holdtime 360
 ip nhrp nhs 10.10.100.100
 ip nhrp registration no-unique
 ip nhrp cache non-authoritative
 ip tcp adjust-mss 1360
 no ip split-horizon eigrp 100
 delay 1000
 tunnel source Vlan30
 tunnel mode gre multipoint
 tunnel key 100355
 tunnel protection ipsec profile SDM_Profile1
interface Tunnel100
        no ip address
        ip pim sparse-mode
interface FastEthernet0/0
```

```
        description to 802.11 G Bridge
        ip address 192.168.100.17 255.255.255.240
        ip mobile foreign-service reverse-tunnel
        ip pim sparse-mode
        ip irdp
        ip irdp maxadvertinterval 10
        ip irdp minadvertinterval 7
        ip irdp holdtime 30
        duplex auto
        speed auto
interface Serial1/0
        no ip address
        shutdown
interface Serial1/1
        no ip address
        shutdown
interface Serial1/2
        no ip address
        shutdown
interface Serial1/3
        no ip address
        shutdown
        clock rate 2000000
interface FastEthernet2/0
        switchport access vlan 10
        duplex half
        speed 100
interface FastEthernet2/1
        switchport mode trunk
        vlan-id dot1q 30
        exit-vlan-config
  vlan-id dot1q 50
  exit-vlan-config
  vlan-id dot1q 60
  exit-vlan-config
  vlan-id dot1q 70
  exit-vlan-config
interface FastEthernet2/2
        switchport access vlan 40
interface FastEthernet2/3
        switchport access vlan 20
interface Vlan1
        no ip address
        shutdown
interface Vlan2
        no ip address
```

```
interface Vlan10
        description to Internet Router
        ip address 58.137.94.206 255.255.255.240
        ip pim sparse-mode
        ip nat outside
        ip virtual-reassembly
interface Vlan20
        description to 802.11G AP
        ip address 192.168.100.81 255.255.255.240
        ip pim dense-mode
        ip nat inside
        ip virtual-reassembly
        crypto map dynmap
interface Vlan30
        description CCTLAN use w switch Red side Fortress
        ip address 192.168.150.1 255.255.255.0 secondary
        ip address 192.168.100.65 255.255.255.240
        ip mobile foreign-service reverse-tunnel
        ip pim dense-mode
        ip nat inside
        ip irdp
        ip irdp maxadvertinterval 10
        ip irdp minadvertinterval 7
        ip irdp holdtime 30
        ip virtual-reassembly
interface Vlan40
        description internal connection to SBC
        ip address 192.168.100.97 255.255.255.240
interface Vlan50
        ip address 192.168.25.1 255.255.255.224
interface Vlan60
        ip address 192.168.25.97 255.255.255.224
interface Vlan70
        ip address 192.168.30.1 255.255.255.0
interface Vlan80
        no ip address
        shutdown
router mobile
router eigrp 100
        redistribute connected
        redistribute static
        redistribute mobile
        network 10.10.100.0 0.0.0.255
        network 192.168.25.0 0.0.0.31
        network 192.168.25.96 0.0.0.31
        network 192.168.30.0
```

```
        network 192.168.40.0
        network 192.168.100.64 0.0.0.15
        network 192.168.100.80 0.0.0.15
        network 192.168.200.0
        no auto-summary
    ip local pool dynpool 192.168.100.101 192.168.100.125
    ip route 0.0.0.0 0.0.0.0 58.137.94.193
    ip route 10.107.0.0 255.255.0.0 192.168.100.67
    no ip http server
    no ip http secure-server
    ip mobile home-agent
    ip mobile virtual-network 192.168.50.0 255.255.255.0
    ip mobile virtual-network 192.168.60.0 255.255.255.0
    ip mobile virtual-network 192.168.55.0 255.255.255.0
    ip mobile host 192.168.50.1 virtual-network 192.168.50.0 255.255.255.0
    ip mobile host 192.168.55.1 virtual-network 192.168.55.0 255.255.255.0
    ip mobile host 192.168.60.1 virtual-network 192.168.60.0 255.255.255.0
    ip mobile mobile-networks 192.168.50.1
     register
     template Tunnel100
    ip mobile mobile-networks 192.168.55.1
     register
     template Tunnel100
    ip mobile mobile-networks 192.168.60.1
     register
     template Tunnel100
    ip mobile foreign-agent care-of Loopback0
    ip mobile secure host 192.168.50.1 spi 100 key ascii TEST algorithm md5 mode
pre
    fix-suffix
    ip mobile secure host 192.168.55.1 spi 120 key ascii TEST algorithm md5 mode
pre
    fix-suffix
    ip mobile secure host 192.168.60.1 spi 110 key ascii TEST algorithm md5 mode
pre
    fix-suffix
    ip pim bidir-enable
    ip pim rp-address 10.10.10.10
    ip nat pool Harkins 58.137.94.206 58.137.94.206 prefix-length 28
    ip nat inside source list 10 pool Harkins overload
    !
    ip access-list extended addr-pool
    !
    snmp-server community nps_flak RO
    control-plane
    line con 0
```

```
        stopbits 1
line aux 0
line vty 0 4
 password cisco
 login
end
```

UAV FLAK (MOBILE NODE OF THE NETWORK)

```
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname UAVFLAKBridge
!
enable secret 5 $1$3nC1$fq3NeJy4RzCgNj/F4NlvB/
!
ip subnet-zero
!
no aaa new-model
!
dot11 ssid AIR1
   authentication open
   guest-mode
!
username Cisco password 7 047802150C2E
!
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 ssid AIR1
 !
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0
 54.0
 station-role non-root bridge
 rts threshold 4000
 infrastructure-client
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface FastEthernet0
 no ip address
```

```
 no ip route-cache
 bridge-group 1
 bridge-group 1 spanning-disabled
 hold-queue 80 in
!
interface BVI1
 ip address 192.168.55.18 255.255.255.240
 no ip route-cache
!
ip http server
no ip http secure-server
ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
!
control-plane
!
bridge 1 route ip
!
line con 0
line vty 0 4
 login local
!
End
```

MIO FLAK (MOBILE NODE OF THE NETWORK)

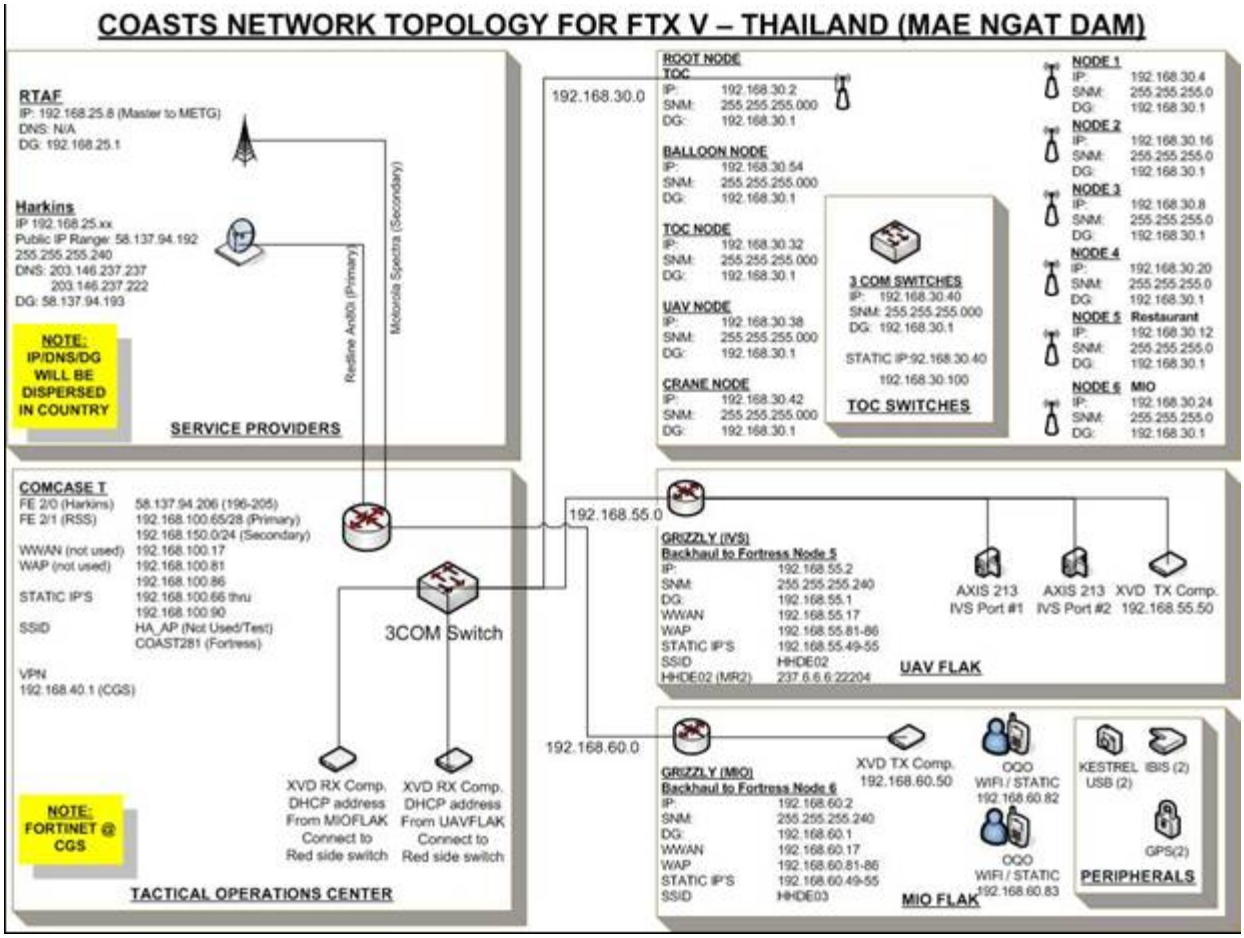
```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname MIOFLAK
!
boot-start-marker
boot system flash c3250-adventerprisek9-mz.124-11.T.bin
boot-end-marker
!
enable password cisco
!
no aaa new-model
ip cef
!
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.60.81 192.168.60.86
ip dhcp excluded-address 192.168.60.49 192.168.60.55
ip dhcp excluded-address 192.168.60.64 192.168.60.70
```

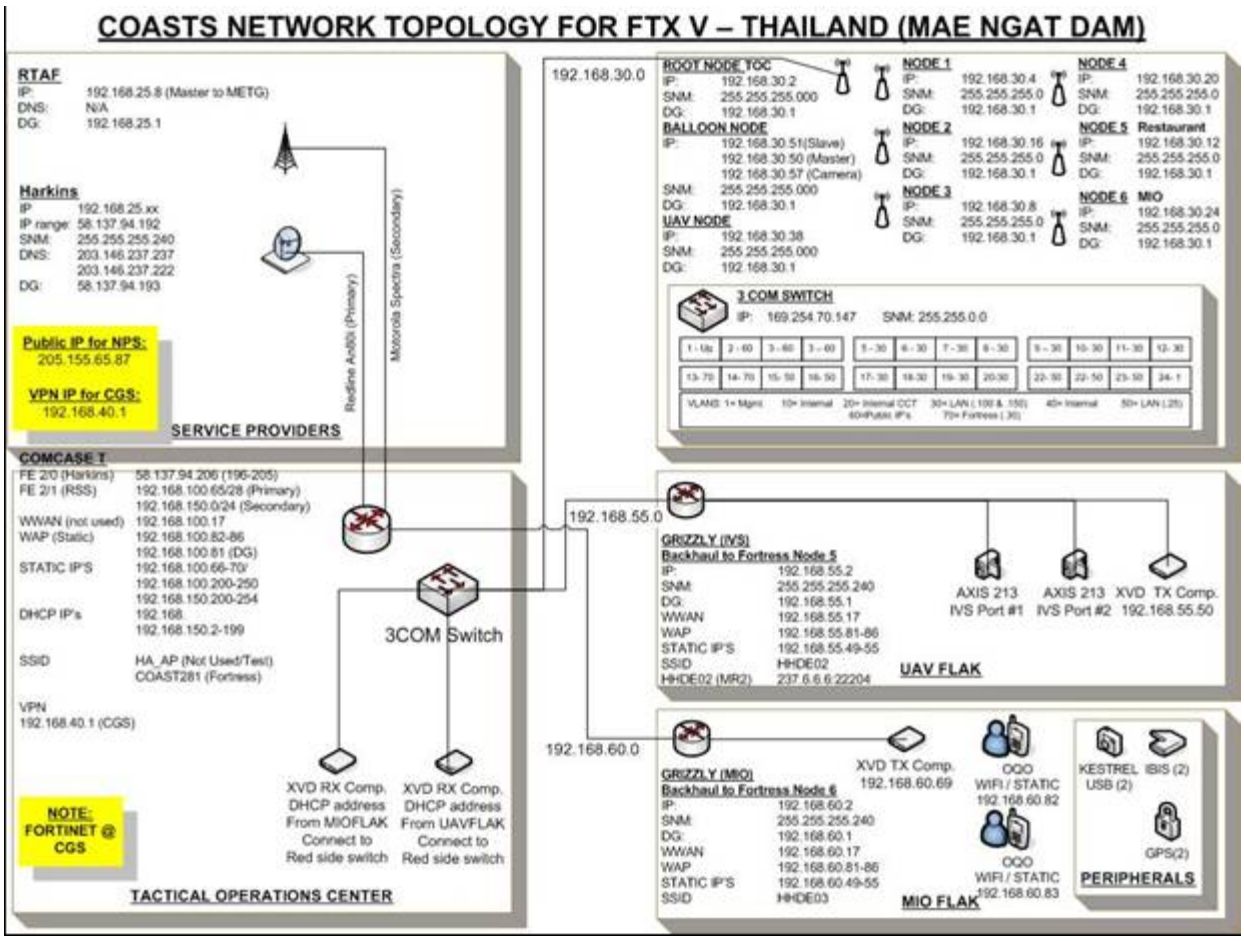
```
!
ip dhcp pool MIOFLAKAP
   network 192.168.60.80 255.255.255.240
   default-router 192.168.60.81
   lease infinite
!
ip dhcp pool MIOFLAKLAN
   network 192.168.60.64 255.255.255.240
   default-router 192.168.60.65
   lease infinite
!
ip multicast-routing
!
multilink bundle-name authenticated
!
no spanning-tree vlan 2
no spanning-tree vlan 3
!
interface Loopback0
 ip address 192.168.60.1 255.255.255.240
 ip pim dense-mode
!
interface Tunnel100
 no ip address
 ip pim sparse-mode
!
interface FastEthernet0/0
 description Connected to 2.4WMIC - Bridge
 ip address 192.168.60.17 255.255.255.240
 ip mobile router-service roam
 ip pim sparse-mode
 duplex auto
 speed auto
 no routing dynamic
!
interface Serial1/0
 no ip address
 shutdown
!
interface Serial1/1
 no ip address
 shutdown
!
interface Serial1/2
 no ip address
 shutdown
```

```
 clock rate 2000000
!
interface Serial1/3
 no ip address
 shutdown
 clock rate 2000000
!
interface FastEthernet2/0
 description 802.16
 switchport access vlan 100
!
interface FastEthernet2/1
 description MIOFLAKLAN
 switchport access vlan 400
!
interface FastEthernet2/2
 description MIOFLAKLAN
 switchport access vlan 400
!
interface FastEthernet2/3
 description 802.11 AP
 switchport access vlan 300
!
interface Vlan1
 ip address 192.168.1.10 255.255.255.0
!
interface Vlan100
 description 802.16
 ip address 192.168.60.49 255.255.255.240
 ip mobile router-service roam priority 200
 ip pim sparse-mode
 no routing dynamic
!
interface Vlan300
 description 802.11 AP
 ip address 192.168.60.81 255.255.255.240
 ip pim dense-mode
!
interface Vlan400
 description MIOFLAKLAN
 ip address 192.168.60.65 255.255.255.240
 ip pim dense-mode
!
router mobile
!
!
```

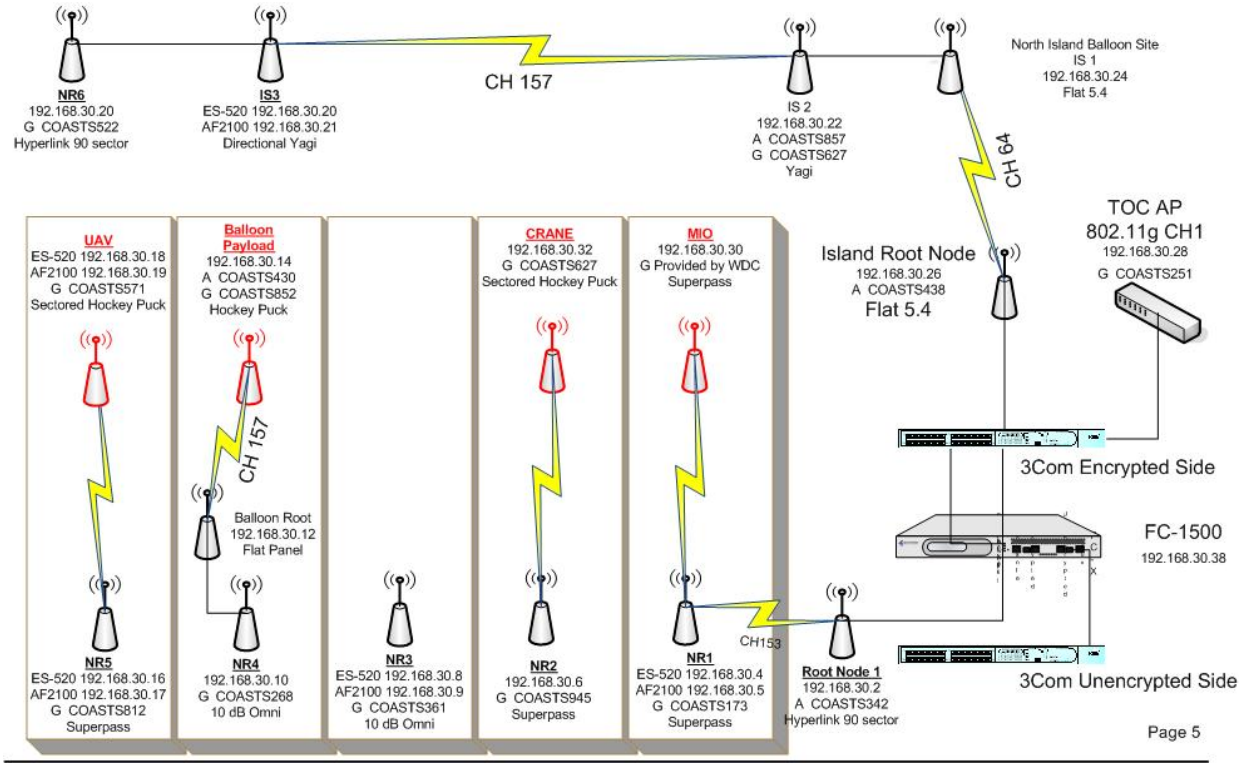
```
!
ip http server
no ip http secure-server
ip mobile secure home-agent 192.168.100.1 spi 110 key ascii TEST algorithm
md5 m
ode prefix-suffix
ip mobile router
 address 192.168.60.1 255.255.255.240
 home-agent 192.168.100.1
 mobile-network Vlan1
 mobile-network FastEthernet0/0
 mobile-network Vlan100
 mobile-network Vlan400
 mobile-network Vlan300
 template Tunnel100
 reverse-tunnel
!
control-plane
!
line con 0
 transport output all
 stopbits 1
line aux 0
 transport output all
line vty 0 4
 password cisco
 login
!
End
```

APPENDIX B – FIELD TRAINING EXERCISE DIAGRAMS

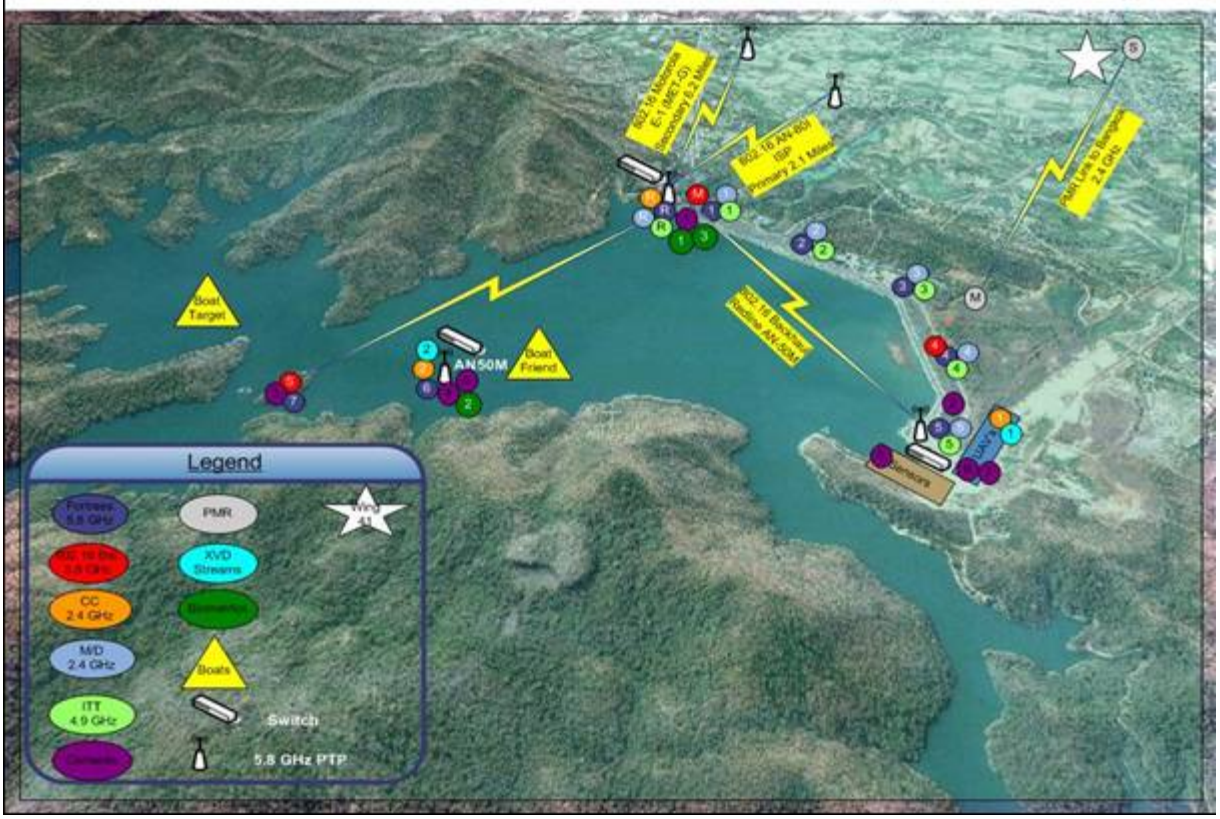



COASTS NETWORK TOPOLOGY FOR FTX V – THAILAND (MAE NGAT DAM)
RTAF
IP: 192.168.25.8 (Master to METG)
DNS: N/A
DG: 192.168.25.1
Harkins
IP 192.168.25.xx
IP range: 58.137.94.192
SNM: 255.255.255.240
DNS: 203.146.237.237
203.146.237.222
DG: 58.137.94.193
Public IP for NPS:
205.155.65.87
VPN IP for CGS:
192.168.40.1
SERVICE PROVIDERS
Redline An80i (Primary)
Motorola Spectra (Secondary)
192.168.30.0
ROOT NODE TOC
IP: 192.168.30.2
SNM: 255.255.255.000
DG: 192.168.30.1
BALLOON NODE
IP: 192.168.30.51(Slave)
192.168.30.50 (Master)
192.168.30.57 (Camera)
SNM: 255.255.255.000
DG: 192.168.30.1
UAV NODE
IP: 192.168.30.38
SNM: 255.255.255.000
DG: 192.168.30.1
NODE 1
IP: 192.168.30.4
SNM: 255.255.255.0
DG: 192.168.30.1
NODE 2
IP: 192.168.30.16
SNM: 255.255.255.0
DG: 192.168.30.1
NODE 3
IP: 192.168.30.8
SNM: 255.255.255.0
DG: 192.168.30.1
NODE 4
IP: 192.168.30.20
SNM: 255.255.255.0
DG: 192.168.30.1
NODE 5 Restaurant
IP: 192.168.30.12
SNM: 255.255.255.0
DG: 192.168.30.1
NODE 6 MIO
IP: 192.168.30.24
SNM: 255.255.255.0
DG: 192.168.30.1
3 COM SWITCH
IP: 169.254.70.147 SNM: 255.255.0.0
COMCASE T
FE 2/0 (Harkins) 58.137.94.206 (196-205)
FE 2/1 (RSS) 192.168.100.65/28 (Primary)
192.168.150.0/24 (Secondary)
WWAN (not used) 192.168.100.17
WAP (Static) 192.168.100.82-86
192.168.100.81 (DG)
STATIC IP'S 192.168.100.66-70/
192.168.100.200-250
192.168.150.200-254
DHCP IP's 192.168.
192.168.150.2-199
SSID HA_AP (Not Used/Test)
COAST281 (Fortress)
VPN
192.168.40.1 (CGS)
192.168.55.0
3COM Switch
GRIZZLY (IVS)
Backhaul to Fortress Node 5
IP: 192.168.55.2
SNM: 255.255.255.240
DG: 192.168.55.1
WWAN 192.168.55.17
WAP 192.168.55.81-86
STATIC IP'S 192.168.55.49-55
SSID HHDE02
HHDE02 (MR2) 237.6.6.6:22204
AXIS 213 IVS Port #1
AXIS 213 IVS Port #2
XVD TX Comp. 192.168.55.50
UAV FLAK
192.168.60.0
GRIZZLY (MIO)
Backhaul to Fortress Node 6
IP: 192.168.60.2
SNM: 255.255.255.240
DG: 192.168.60.1
WWAN 192.168.60.17
WAP 192.168.60.81-86
STATIC IP'S 192.168.60.49-55
SSID HHDE03
XVD TX Comp. 192.168.60.69
OQO WIFI / STATIC 192.168.60.82
OQO WIFI / STATIC 192.168.60.83
MIO FLAK
KESTREL USB (2)
IBIS (2)
GPS(2)
PERIPHERALS
XVD RX Comp. DHCP address From MIOFLAK Connect to Red side switch
XVD RX Comp. DHCP address From UAVFLAK Connect to Red side switch
NOTE: FORTINET @ CGS
TACTICAL OPERATIONS CENTER

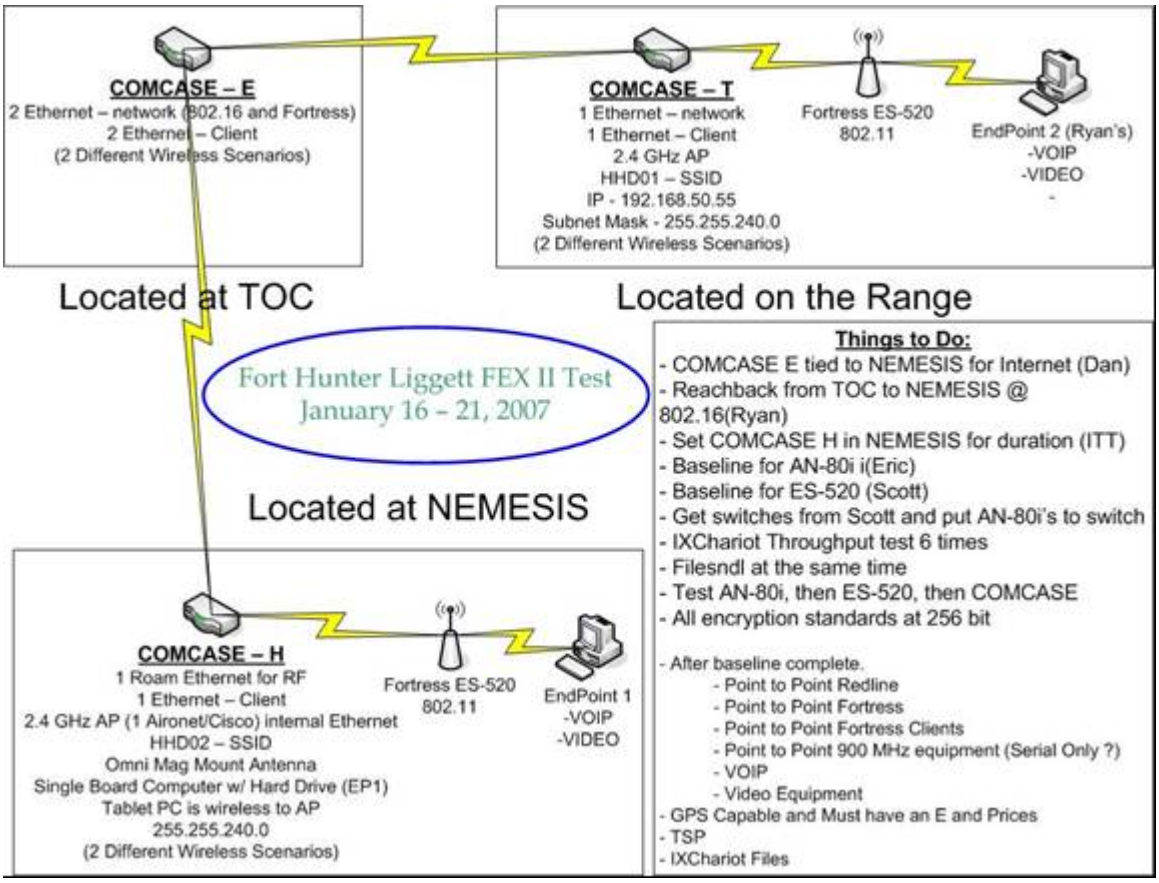
Fortress Network COASTS Thailand May Event
ES-520
Friday, May 25, 2007

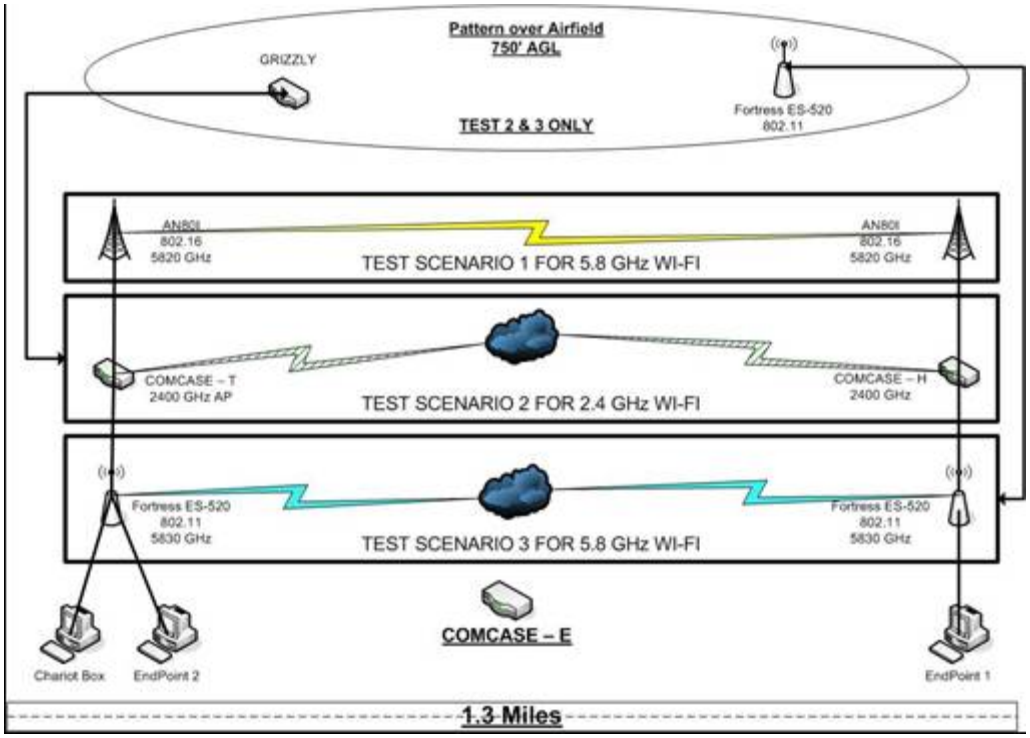


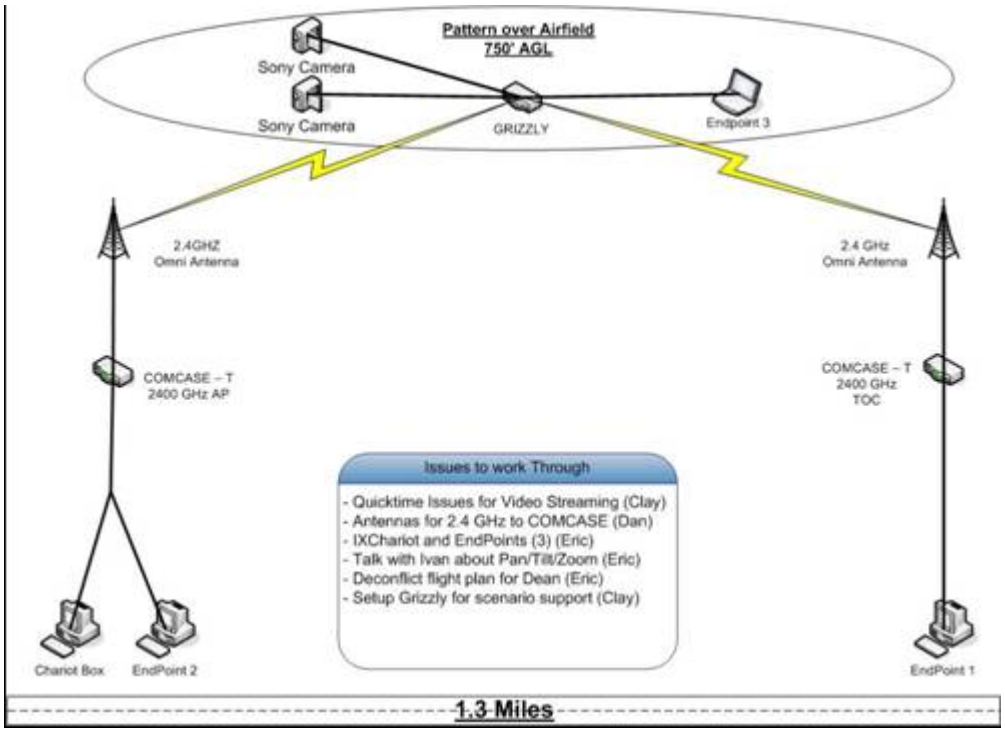
COASTS NETWORK TOPOLOGY FOR FTX V – THAILAND (MAE NGAT DAM)

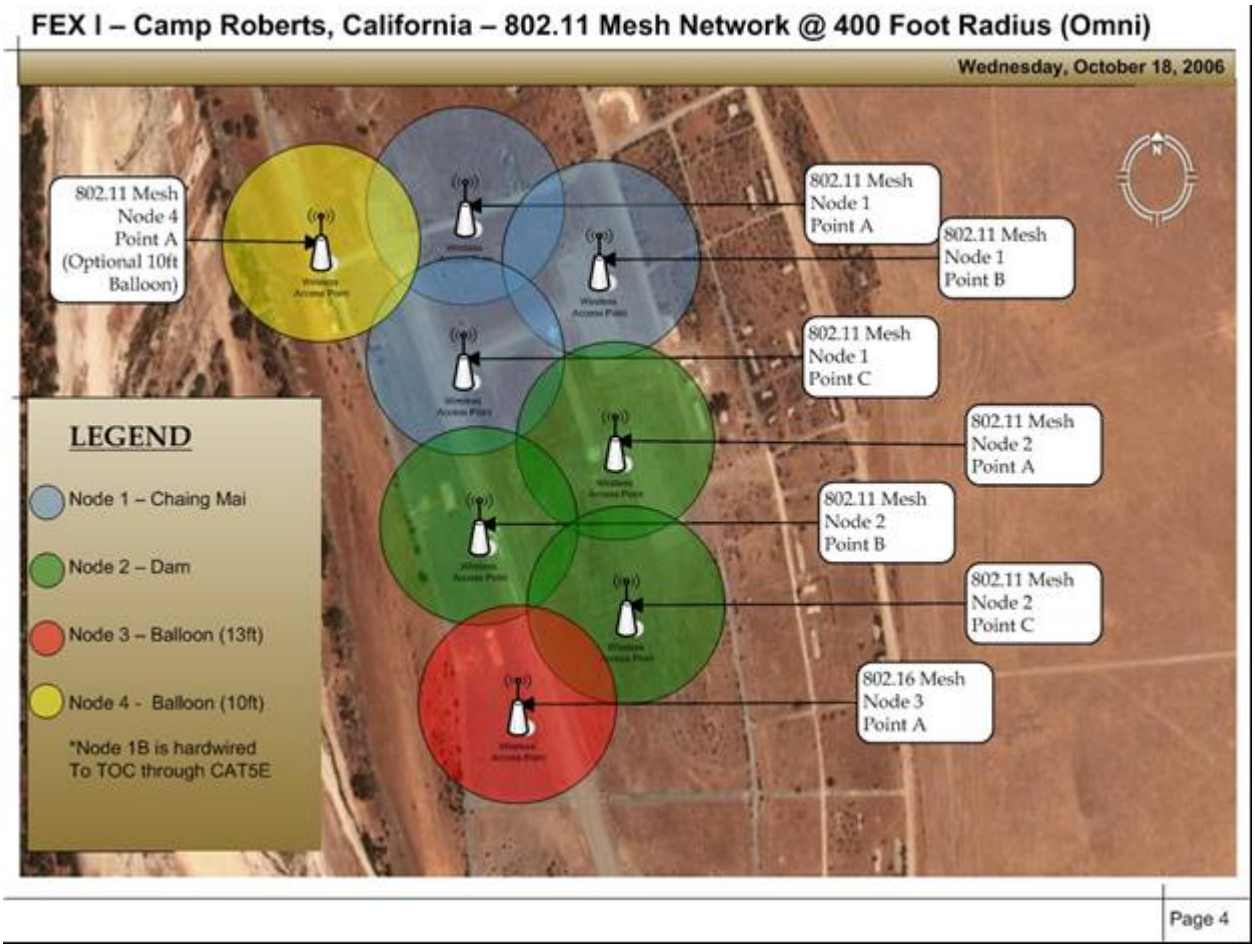


APPENDIX C – FIELD EXERCISES

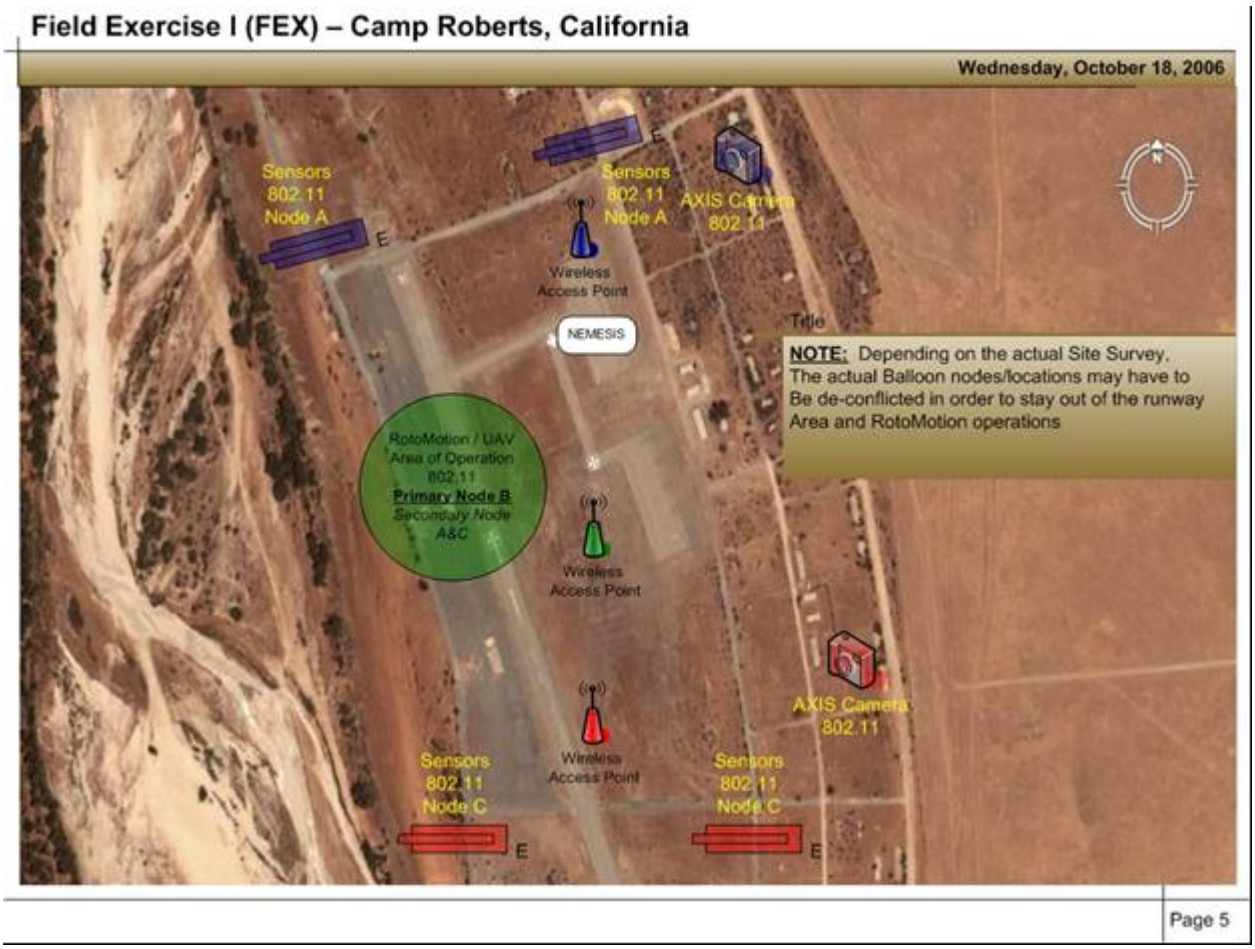

COMCASE – E
2 Ethernet – network (802.16 and Fortress)
2 Ethernet – Client
(2 Different Wireless Scenarios)
COMCASE – T
1 Ethernet – network
1 Ethernet – Client
2.4 GHz AP
HHD01 – SSID
IP - 192.168.50.55
Subnet Mask - 255.255.240.0
(2 Different Wireless Scenarios)
Fortress ES-520
802.11
EndPoint 2 (Ryan's)
-VOIP
-VIDEO
Located at TOC
Located on the Range
Fort Hunter Liggett FEX II Test
January 16 – 21, 2007
Located at NEMESIS
Things to Do:
- COMCASE E tied to NEMESIS for Internet (Dan)
- Reachback from TOC to NEMESIS @ 802.16(Ryan)
- Set COMCASE H in NEMESIS for duration (ITT)
- Baseline for AN-80i i(Eric)
- Baseline for ES-520 (Scott)
- Get switches from Scott and put AN-80i's to switch
- IXChariot Throughput test 6 times
- Filesndl at the same time
- Test AN-80i, then ES-520, then COMCASE
- All encryption standards at 256 bit
- After baseline complete.
- Point to Point Redline
- Point to Point Fortress
- Point to Point Fortress Clients
- Point to Point 900 MHz equipment (Serial Only ?)
- VOIP
- Video Equipment
- GPS Capable and Must have an E and Prices
- TSP
- IXChariot Files
COMCASE – H
1 Roam Ethernet for RF
1 Ethernet – Client
2.4 GHz AP (1 Aironet/Cisco) internal Ethernet
HHD02 – SSID
Omni Mag Mount Antenna
Single Board Computer w/ Hard Drive (EP1)
Tablet PC is wireless to AP
255.255.240.0
(2 Different Wireless Scenarios)
Fortress ES-520
802.11
EndPoint 1
-VOIP
-VIDEO

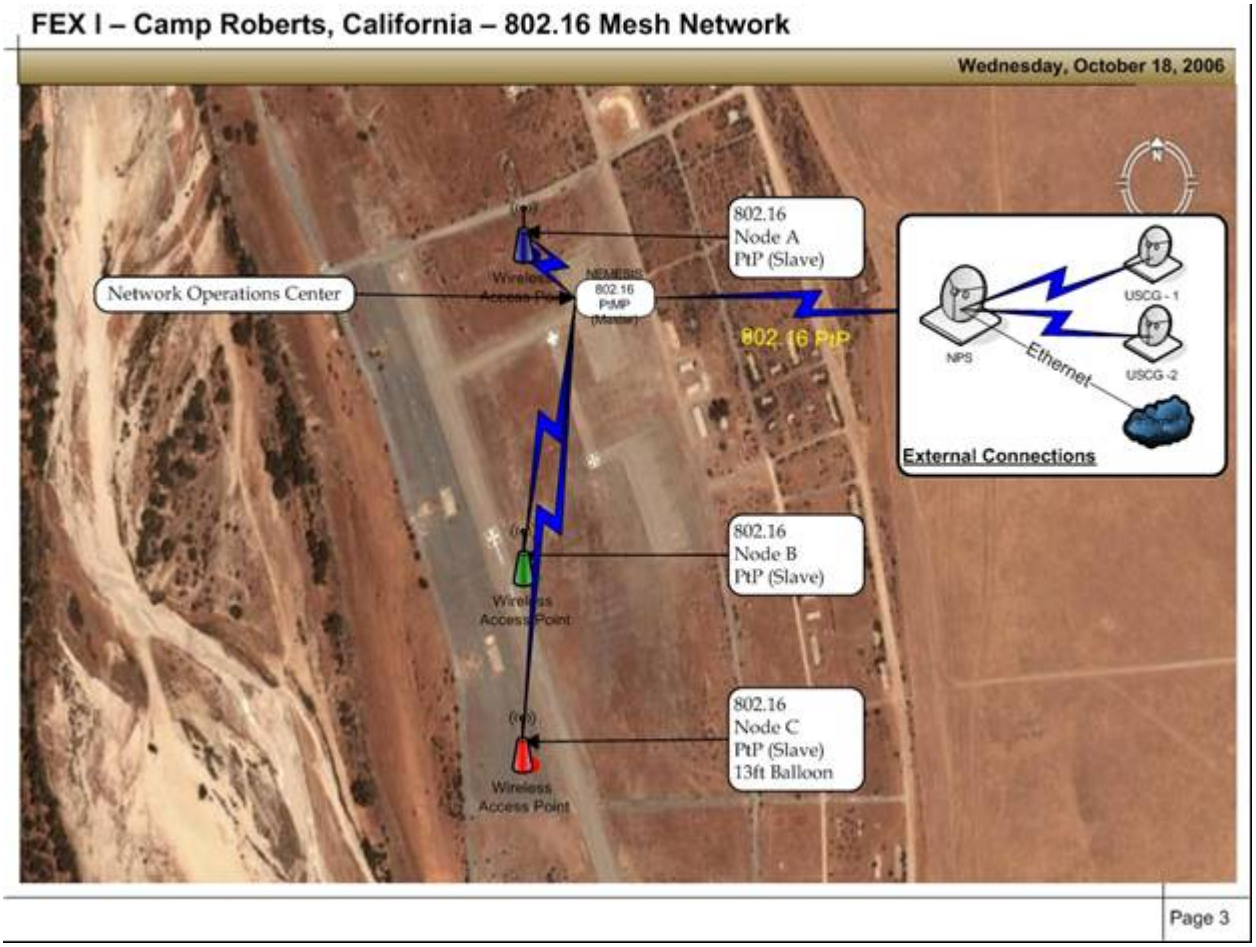

Pattern over Airfield
750' AGL
GRIZZLY
Fortress ES-520
802.11
TEST 2 & 3 ONLY
AN80i
802.16
5820 GHz
TEST SCENARIO 1 FOR 5.8 GHz WI-FI
AN80i
802.16
5820 GHz
COMCASE – T
2400 GHz AP
TEST SCENARIO 2 FOR 2.4 GHz WI-FI
COMCASE – H
2400 GHz
Fortress ES-520
802.11
5830 GHz
TEST SCENARIO 3 FOR 5.8 GHz WI-FI
Fortress ES-520
802.11
5830 GHz
COMCASE – E
Chariot Box
EndPoint 2
EndPoint 1
1.3 Miles

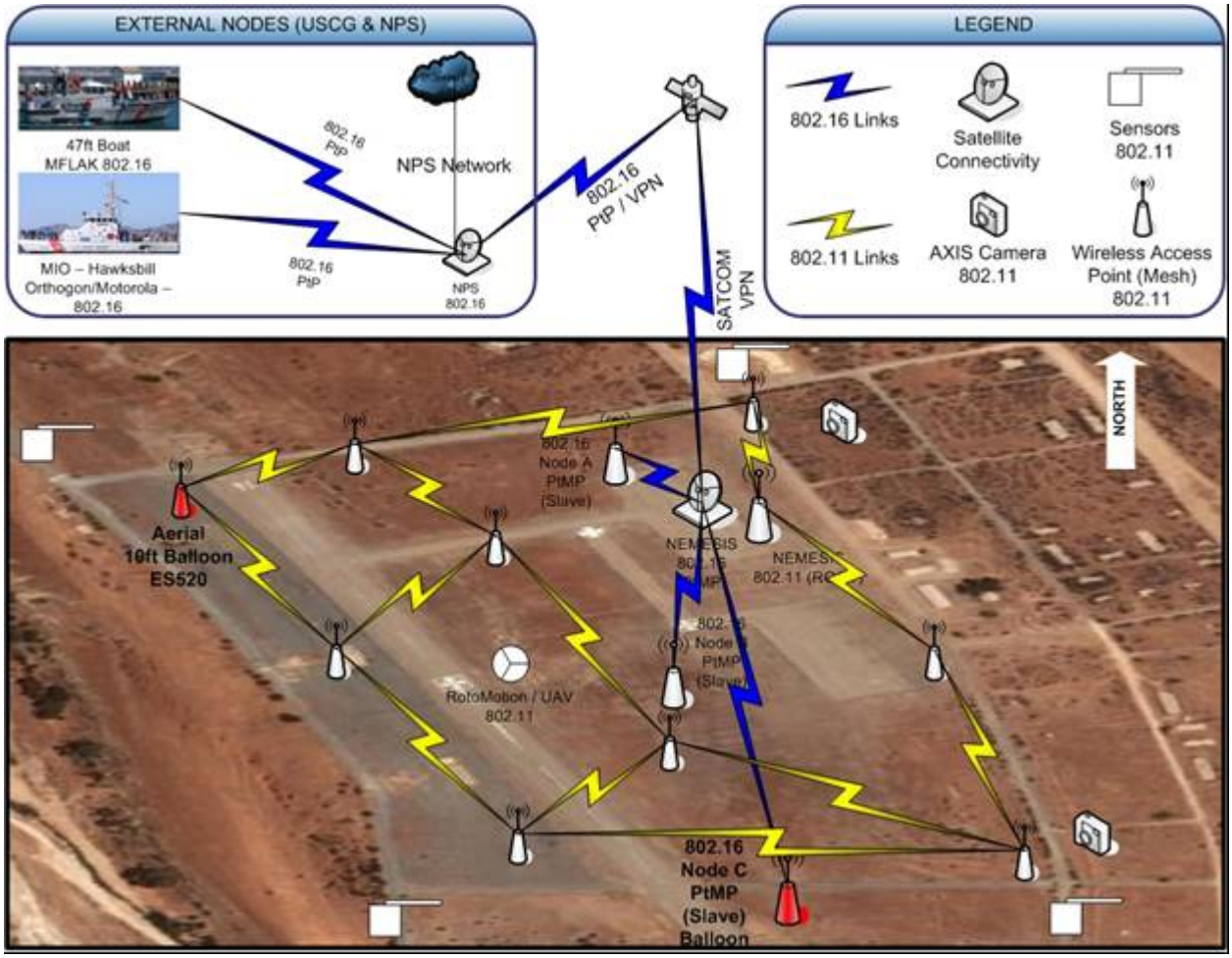

Pattern over Airfield
750' AGL
Sony Camera
Sony Camera
GRIZZLY
Endpoint 3
2.4GHZ
Omni Antenna
2.4 GHz
Omni Antenna
COMCASE – T
2400 GHz AP
COMCASE – T
2400 GHz
TOC
Issues to work Through
- Quicktime Issues for Video Streaming (Clay)
- Antennas for 2.4 GHz to COMCASE (Dan)
- IXChariot and EndPoints (3) (Eric)
- Talk with Ivan about Pan/Tilt/Zoom (Eric)
- Deconflict flight plan for Dean (Eric)
- Setup Grizzly for scenario support (Clay)
Chariot Box
EndPoint 2
EndPoint 1
1.3 Miles

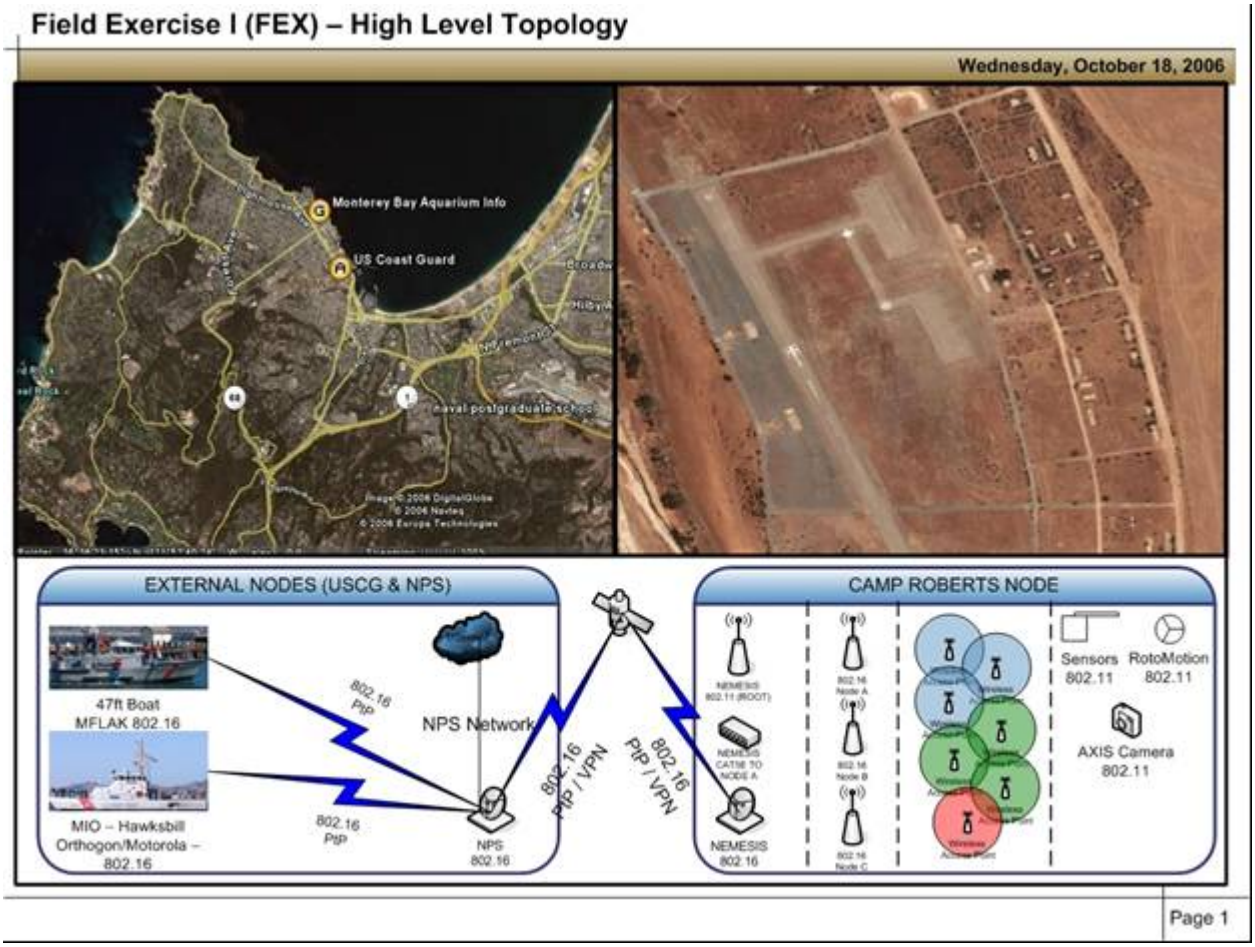

FEX I – Camp Roberts, California – 802.11 Mesh Network @ 400 Foot Radius (Omni)
Wednesday, October 18, 2006
802.11 Mesh Node 4 Point A (Optional 10ft Balloon)
802.11 Mesh Node 1 Point A
802.11 Mesh Node 1 Point B
802.11 Mesh Node 1 Point C
802.11 Mesh Node 2 Point A
802.11 Mesh Node 2 Point B
802.11 Mesh Node 2 Point C
802.16 Mesh Node 3 Point A
LEGEND
Node 1 – Chaing Mai
Node 2 – Dam
Node 3 – Balloon (13ft)
Node 4 - Balloon (10ft)
*Node 1B is hardwired To TOC through CAT5E
Page 4

Field Exercise I (FEX) – Camp Roberts, California




FEX I – Camp Roberts, California – 802.16 Mesh Network
Wednesday, October 18, 2006
Network Operations Center
Wireless Access Point
MEMESIS
802.16 PtMP (Master)
802.16 Node A PtP (Slave)
802.16 PtP
NPS
Ethernet
USCG - 1
USCG -2
External Connections
802.16 Node B PtP (Slave)
Wireless Access Point
802.16 Node C PtP (Slave) 13ft Balloon
Wireless Access Point
Page 3


EXTERNAL NODES (USCG & NPS)
47ft Boat
MFLAK 802.16
MIO – Hawksbill
Orthogon/Motorola –
802.16
802.16
PtP
802.16
PtP
NPS Network
NPS
802.16
802.16
PtP / VPN
SATCOM
VPN
LEGEND
802.16 Links
Satellite
Connectivity
Sensors
802.11
802.11 Links
AXIS Camera
802.11
Wireless Access
Point (Mesh)
802.11
NORTH
802.16
Node A
PtMP
(Slave)
Aerial
10ft Balloon
ES520
NEMESIS
802.16
PtMP
NEMESIS
802.11 (RC
802.16
Node B
PtMP
(Slave)
RotoMotion / UAV
802.11
802.16
Node C
PtMP
(Slave)
Balloon


Field Exercise I (FEX) – High Level Topology
Wednesday, October 18, 2006
Monterey Bay Aquarium Info
US Coast Guard
naval postgraduate school
EXTERNAL NODES (USCG & NPS)
47ft Boat
MFLAK 802.16
MIO – Hawksbill
Orthogon/Motorola –
802.16
802.16
PtP
802.16
PtP
NPS Network
NPS
802.16
802.16
PtP / VPN
802.16
PtP / VPN
CAMP ROBERTS NODE
NEMESIS
802.16
Sensors
802.11
RotoMotion
802.11
AXIS Camera
802.11
Page 1

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D – COTS TECHNICAL SPECIFICATIONS

Redline Communications AN-50 E/M - IEEE 802.16 Radio

System Capability: LOS, optical-LOS, and non-LOS (OFDM)
RF Band: 5.470-5.850 GHz, TDD
Channel Size: 20 MHz (5 MHz steps)
Data Rate: Up to 49 Mbps average Ethernet rate
Max TX Power: 20 dBm (region specific)
Rx Sensitivity: -86 dBm @ 6 Mbps (BER of 1x10e-9)
IF Cable: Up to 228 m (750 ft)
Network Attributes: Transparent bridge, automatic link distance ranging1, 802.3x1, 802.1p1, DHCP pass-through, 802.1Q VLAN2, encryption
Modulation: BPSK to 64 QAM (bidirectional dynamic adaptive), Dynamic Channel Control: DFS, ATPC
MAC: PTP, PMP, concatenation/fragmentation, ARQ
Range: Beyond 80 km (50 mi) LOS @ 48 dBm EIRP
Network Connection: 10/100 Ethernet (RJ-45)
System Configuration: HTTP (Web) interface, SNMP, CLI, console (RS-232)
Network Management: SNMP: standard/proprietary MIBs
Power: 110-240 VAC 50/60 Hz, 18-72 VDC, dual
Compliance: EN 60950, EN 301 893, EN 301 390, EN 301 489-1 & 17, FCC part 15

Redline Communications AN-80i – IEEE 802.16 Radio
System Capability: LOS, Optical-LOS, and Non-LOS
RF Band: 5.725 GHz to 5.850 GHz (TDD)
Center Frequency Steps: 2.5 MHz 1
Channel Size: 10/20/40 MHz (software selectable)
RF Dynamic Range: > 50 dB
Data Rate: Up to 48 Mbps average Ethernet rate (20 MHz channel) 2
Up to 90 Mbps average Ethernet rate (40 MHz channel) 2
Ave. TX Mode Power: Max. +20 dBm (region specific)3
Rx Sensitivity: -82 dBm @ 6 Mbps (based on BER of 1x10e-9)
PoE Cable: Up to 91 m (300 ft) 4
Network Attributes: 802.1p network traffic prioritization
802.3x Ethernet flow control
Automatic link distance ranging
DHCP pass-through, Transparent bridge
Automatic Transmit Power Control (ATPC)
Modulation/Coding Rates: Adaptive Modulation (bi-directional burst to burst) auto selects: 1/2 BPSK, 3/4 BPSK, 1/2 QPSK, 3/4 QPSK, 1/2
16 QAM, 3/4 16 QAM, 2/3 64 QAM and 3/4 64 QAM
Over The Air Encryption: 64-bit private key encryption
MAC: PTP deployment, concatenation
Time Division Multiple Access (TDMA)

Automatic Repeat Request (ARQ) error correction
Dynamic adaptive modulation (BPSK to 64 QAM)
Range: Up to 80 km (50 mi) line-of-sight @ 48 dBm EIRP
Network Services: Transparent to 802.3 services and applications
Duplex Technique: Dynamic TDD (time division duplex)
Wireless Transmission: OFDM (orthogonal frequency division multiplexing)
Network Connection: 10/100 Ethernet (RJ-45)
System Configuration: HTTP (Web) interface, SNMP, Telnet/CLI
Network Management: SNMP: standard and proprietary MIBs
Power Requirements: Standard IEEE 802.3af (15.4 W Max.)
Compliance: Safety: IEC, EN, and UL/CSA 60950
EMC: 301 489-1, 301 489-17
5.8 GHz Radio: Industry Canada RSS 210, FCC part 15,
ETSI EN 302 502 (pending)
Operating Temperature: Operating Cond.: -40 C to 60 C
Dimensions/Weight: 289 mm x 190 mm x 515 mm (11.38 in x 7.50 in x 2.03 in)
Humidity: 0% to 90% Non-condensing
Weight: 2 Kg (4.4 lb) without bracket or antenna
PoE Power Block: CINCON Model TR60A-POE-L
Input: Auto-sensing 110/220/240 VAC 50/60 Hz
Output: Standard IEEE 802.3af

1 Center frequency is dependent on region.
2 Actual Ethernet data throughput is dependent on: protocols, packet size, burst rate, transmission latency, and link distance.
3 In some countries outside of North America, the maximum operational power per channel with
a given antenna is limited in accordance to maximum allowable EIRP levels for the region.
4 With lightning arrestor installed.
Specifications are subject to change without notice.

Fortress Technologies ES-520 - IEEE 802.11 Radio

Range: Tested up to 32 miles (directional antenna), tested up to 7 miles (omni-directional antenna)
Performance: Up to 100 secure clients encryption for AES-128, 192, 256, WPA2 authentication, internal or external RADIUS, PKI/CAC user and device
management • secure browser-based GUI, CLI or SNMP
SSID support • up to 4 SSIDs
Enclosure: Rugged .125" aluminum, NEMA 4 mounting, mast mounting kit and weatherizing kit included
Dimensions: 2.3"H x 8.75"W x 6.6"D, (5.8cm x 22.2cm x 16.8cm)
Weight: 3.46 lbs. (1.57 kg)
Connections: Eight RJ-45 10/100 LAN ports with auto-MDIX
- one RJ-45 10/100 WAN port with PoE receiver
- one RJ-45 serial console port

- two USB ports for future functionality

Radios: one 200 mW 802.11a/b/g radio (maximum transmit power 23dBm) and one 400 mW 802.11a radio (maximum transmit power 26dBm)
Antenna support: 2 N-style external antenna connectors (female)
Radio modes of operation: Wireless access point or bridge
Power supply: External AC-DC power adapter (48V), or PoE and polarity protection
Power draw: 13W maximum
Port LED's: link, activity, status, PoE
Radio LED's: strength and association
Cooling: Convection (no fans)
Operating temperature: -10 ~ 50°C
Humidity: 5 ~ 95%
Weather resistance: Water-resistant front panel cover plate included with: IP56, lightning arrestor, vibration, bounce & shock
MIL-STD 810F
Safety & emissions: CE, FCC, UL 60950-1, IEC 60529 (CB Test), UL(NEMA) 4, NIST, FIPS 140-2 level 2 submitted, EAL 3 submitted

COMCASE H Mobile Router with Home Agent

WDC IPE-10M Coalition Strength AES 256 bit CM Encryptor
Tactical Mobile Router Kit

1– Cisco 3200MAR
2– Cisco 3201FESMIC: Ethernet ports for external notebooks
2/4– Cisco 3201SMIC: Serially interface card for
KU SATCOM and other serial devices
2– Cisco 3201WMIC WiFi: 1– WiFi (AP) and
1–WiFi (Bridge) 2.4 & 4.9 G HZ

MobileCom Cellular Modem: CDMA (1xRTT, EV-DO, HSDPA)
GPS Card (Also a part of cellular modems)
Intelligent Video Server for 2 Analog Video inputs
Single Board Computer with 30 Gig hard drive
Windows/Linux OS
IPICS—RF over VOIP
Call Manager and Voice over IP (VOIP)
BGAN Antenna for SATCOM connectivity
PCMCIA carrier for supporting the SECNET 11 and the Type 1 TALCON PC Cards

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX E - THAILAND FIELD TEST EXERCISE

Introduction

The OCONUS Test in the general area of Mae Ngat Dam in Thailand is a precursor to the demonstrations scheduled in May - June 2007. The overall scenario for COASTS 2007 demonstration involves the transportation of a simulated radiological "dirty bomb," procured with the proceeds of illegal narcotics smuggling, from Myanmar across the border of Thailand. The *bomb* is then transported through Thailand by private vehicle to the south west coast port of Ranong, where it is then loaded on a commercial ship for its onward transit through the Strait of Malacca between Malaysia and Indonesia, across the Pacific Ocean for its final destination as Hawaii. Within this context, there is a requirement to test and evaluate technical and operational components during field testing exercises scheduled to be conducted at Mae Ngat Dam, Thailand. COASTS Team will take this opportunity to deploy, integrate and test all their technologies and prepare themselves for the following demonstrations. The aim of drafting this scenario is to help enable all personnel involved in the experiments to integrate their respective technologies into a more realistic operational environment and allow the technologies to be evaluated within a specific time and event-bound plan.

Salient Parameters for Mae Ngat Dam Scenario

The following parameters have been visualized for developing the scenario for the 19-30 March COASTS Test at Mae Ngat Dam:

- The main objectives of the overall COASTS 2007 scenario will be rehearsed and refined.
- The scenario itself is designed to be simple and flexible to allow assessment of various technologies integrated as part of the COASTS field experimentation project.
- For a more realistic assessment, a Red Team simulating adversary capability and carrying out actions that need to be detected and acted upon by the COASTS team (Blue Team) will be earmarked. The Red Team will also be given certain limits to conduct their respective actions.

Scenario Players

- **Blue Team**: The Blue Team will include all COASTS faculty, students, ONR reservists, and commercial partners involved with technology demonstration and integration, as well as personnel comprised of various military and law enforcement organizations that have a vested interest in the technologies presented by the COASTS field experimentation program.

- **Red Team**: The Red Team will be comprised of a few dedicated personnel who will play the part of rogue elements, whose activities need to be detected by the Blue Team that will then lead to their apprehension and possible interdiction.

- **Control Team**: The Control Team will be comprised of key COASTS personnel responsible for steering and evaluating the Test, from both the Blue Team and the Red Team perspective. This team will be located at the Tactical Operational Center

(TOC), and will be responsible for directing the entire scenario. The Control Team will also include representatives from the Royal Thailand Armed Forces.

Mae Ngat Dam Scenario: Area of Operations

The area of operations for the Test scenario will be in and around the general area of the Mae Ngat Dam, specific boundaries will be identified on ground by the Program Manager in consultation with the Thai authorities.

Figure 1: Mae Ngat Dam Test Scenario – Area of Operations

Figure 2: Mae Ngat Dam Test Scenario – TOC Location

Boundary Depiction

The Test Scenario illustrates two fictitious countries Blue Land and the Red Land in the area of operations. The International Boundary (IB) between the Blue Land and Red Land runs along the Northern edge of the Mae Ngat Dam reservoir from East to West, heads South West from the dam face as depicted in Figure 3 below. Blue Land is to the South and East of the IB and Red Land is to the North and West.

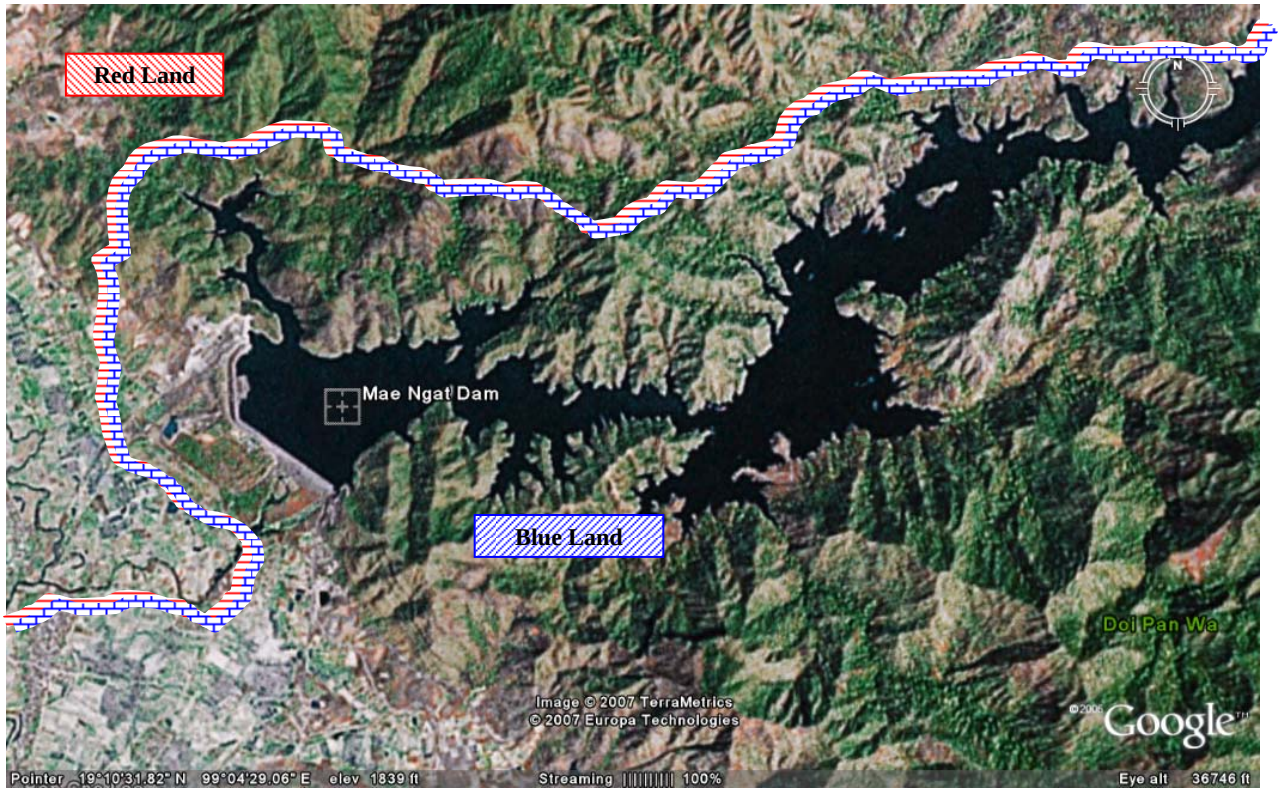


Figure 3: Test Scenario – Boundary Depiction: Blue Land and Red Land

General Description

Blue Land is a stable democratic country that is slowly but steadily emerging on the world stage due to rapid economic progress in the recent times. Blue Land shares its borders with Red Land to the North and West. Red Land is going through internal political turmoil that is accompanied by social and economic unrest. Blue Land has a coastline of approximately 250 miles on its southern side. The instability in and around Blue Land is beginning to spread into its bordering regions and is being covertly supported by Red Land in the West, with an intention of destabilizing Blue Land. Red Land is the country to the North and West of Blue Land and is being ruled by a military dictator. Another major reason for the internal turmoil in Red Land is the growing influence of Harruki fundamentalism within the country. The Red Land military is in full control of the country but has been unable to control the Harruki factions within the society. The Harruki movement within Red Land has started to manipulate the population in the border region of Blue Land and have gained substantial supporters to their beliefs and teachings. A final destabilizing influence is the proliferation of illegal narcotics smuggling into and through Blue Land, much of the traffic originating from inside Red Land.

Taking advantage of the internal turmoil in Red Land, a Harruki fundamentalist Red Team has managed to tie into narcotics smuggling funding sources and fabricate a “dirty bomb” that it now intends to transport through Blue Land to reach a coastal city to the south of Blue Land for its onward transportation to the intended target country through a commercial cargo ship.

The Red Team will initially try and infiltrate Blue Land on foot through the porous borders or by using vehicle transport through one of the many border security check posts. Blue Land Border Security Force has recently upgraded its border surveillance and reconnaissance capabilities through the deployment of state-of-the-art unattended air, land, and sea-based sensors integrated through modern communication network, in an effort to better protect Blue Land borders and prevent the influx of Harruki militants to Blue Land.

Blue Land is also facing a crisis due to flooding that has taken place due to incessant rain. The Blue Land civil authorities in the area of Mae Ngat Dam are providing relief and rehabilitation to the population that has been displaced by floods. The civil authorities have also requested the Blue Land Forces in the area to assist in humanitarian operations that includes search and rescue missions, and for aerial reconnaissance of the flooded area, so that a correct assessment of the humanitarian effort required could be undertaken.

Initial Disposition – Blue Land Forces

Blue Land forces are deployed in the area of operations with an aim to maintain the sanctity of the IB by limiting the influx of the Harruki militants. The area of operations has a TOC, a UAV base, Border Check Posts (BCPs) and a number of Sensor sub-units.

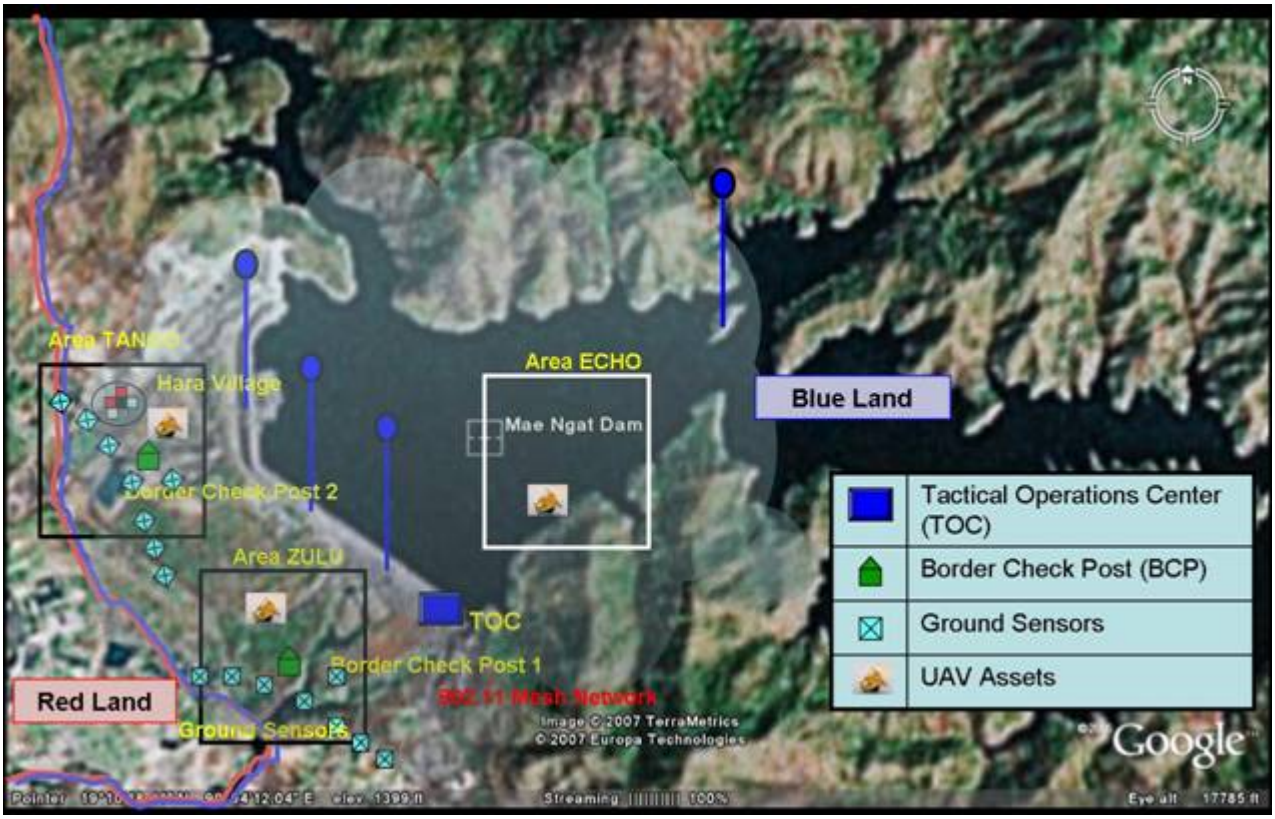


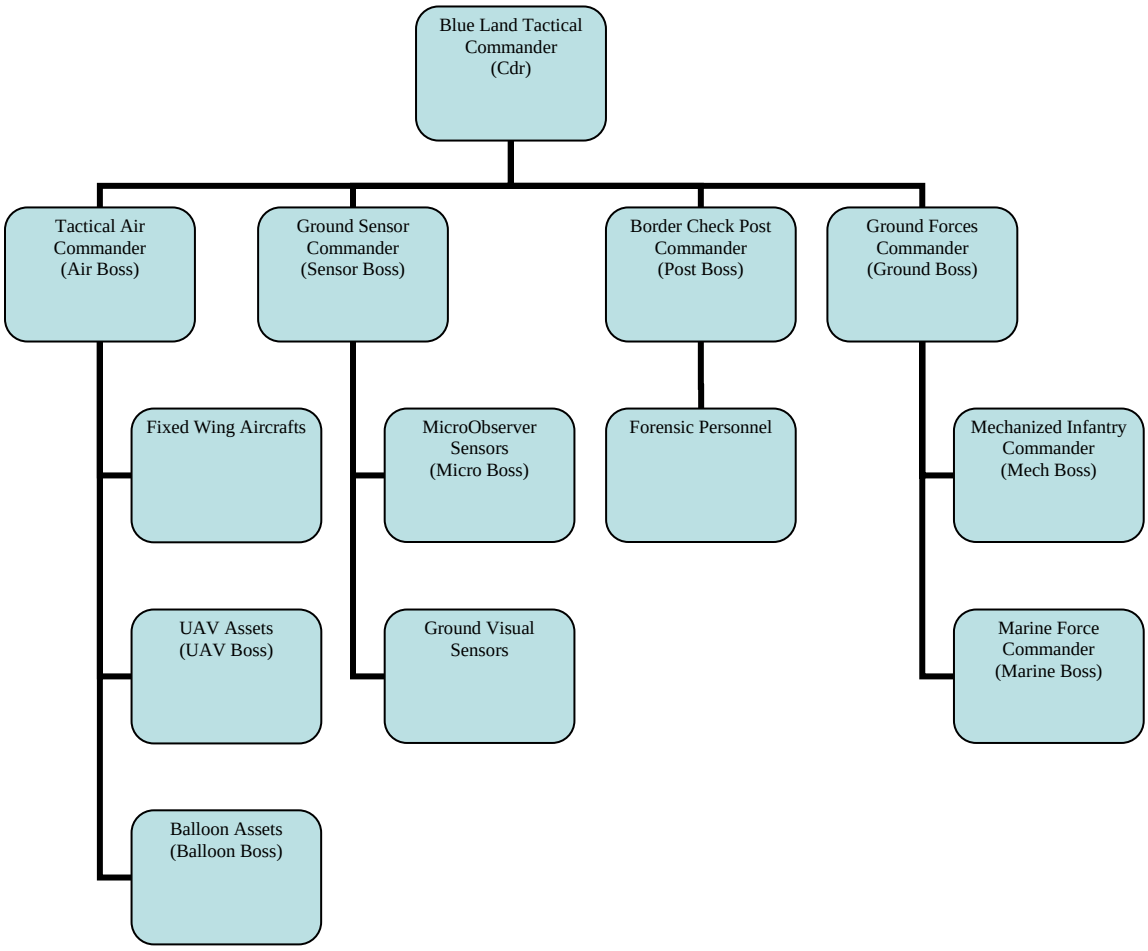
Figure 4: Test Scenario – Initial Disposition of Blue Land Forces in the Area of Operations

Two major sensitive areas – Area ZULU and Area TANGO are present in the area of operations. These are the areas that are likely to be used as infiltration routes by the Harruki militants. The Blue Forces TOC at the Mae Ngat Dam area is commanded by a Tactical Commander (Cdr) who is responsible for all the assets deployed in the area of operations, which includes UAVs, BCPs and the overall surveillance grid established through the use of state-of-the-art sensors. In addition, Blue Land Commander at the Mae Ngat area also has a dedicated Air Force Flight under his command.

Area ECHO as depicted in Figure 4, is earmarked as a flood ravaged area for the purpose of the Test Scenario, the civil administration is likely to request the TOC Cdr for humanitarian support in this area.

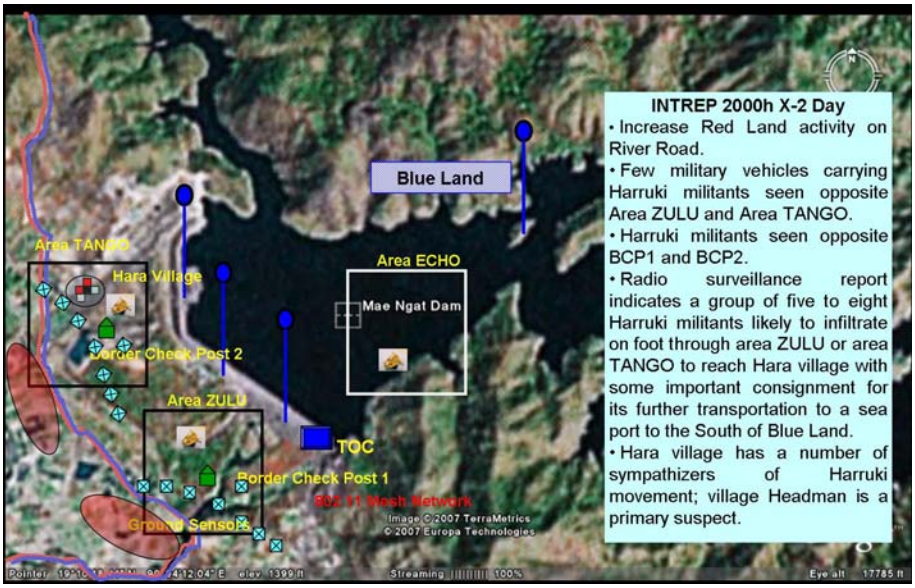
In addition to the TOC, the Blue Land has a Command and Control (C2) Center located at the Interagency Intelligence Fusions Center (IIFC) in its southern city of Chiang Mai and a remote C2 Center at the Blue Land Air Force Headquarters in its capital city of Bangkok.

Command Structure – Blue Land Forces


Blue Land Tactical Commander (Cdr)
Tactical Air Commander (Air Boss)
Ground Sensor Commander (Sensor Boss)
Border Check Post Commander (Post Boss)
Ground Forces Commander (Ground Boss)
Fixed Wing Aircrafts
MicroObserver Sensors (Micro Boss)
Forensic Personnel
Mechanized Infantry Commander (Mech Boss)
UAV Assets (UAV Boss)
Ground Visual Sensors
Marine Force Commander (Marine Boss)
Balloon Assets (Balloon Boss)

Detailed Scenario Description

Time	Event Description and Action	Remarks
2000h X-2 Day	**INTREP Received at TCC**	X Day is the day of commencement of exercise.


INTREP 2000h X-2 Day
• Increase Red Land activity on River Road.
• Few military vehicles carrying Harruki militants seen opposite Area ZULU and Area TANGO.
• Harruki militants seen opposite BCP1 and BCP2.
• Radio surveillance report indicates a group of five to eight Harruki militants likely to infiltrate on foot through area ZULU or area TANGO to reach Hara village with some important consignment for its further transportation to a sea port to the South of Blue Land.
• Hara village has a number of sympathizers of Harruki movement; village Headman is a primary suspect.
Blue Land
Area TANGO
Hara Village
Area ECHO
Mae Ngat Dam
Border Check Post 2
Area ZULU
TOC
Border Check Post 1
Ground Sensors

Scenario – Part I – Operations in Area ZULU

0830h X Day	**BCP 1 SITREP** **Post Boss** - BCP1 reports unusual movement of unidentified persons from the Red Land moving towards the IB.	
0835h X Day	**Cdr** – Air, Sensor, Post and Ground Boss – all alert – provide 30 minutes update on latest situation. **Cdr** – Air Boss, its time to get your assets in the air to get a better picture of the situation in ZULU sector.	
0836h X Day	**Air Boss** – UAV Boss – Execute launch bird immediately and proceed to ZULU sector and loiter on station until further notice. Ensure video surveillance commences when bird is on station.	
0838h X Day	**UAV Boss** – UAV Boss to Air Boss, cope all, stand by while bird is launched...bird is away, proceeding to sector ZULU, will advise when bird is on station. Video feed to commence immediately.	
0840h X Day	**Air Boss** - Balloon Boss – zoom in cameras to GR _____ to detect Harruki.	Video feed of UAV available at TCC.
0841h X day	**Balloon Boss** – Cameras tilted to cover GR _____, forwarding live feed to TCC now.	Video feed available at TCC from both UAV and Balloon cameras.
0842h X Day	**Control Team** - Red Team located opposite ZULU sector, commence movement from Start Point - GR _____ to Finish Point - GR _____ to move towards IB. Use available local camouflage during move. Switch on APRS tracker immediately.	Movement of Red Team now available at TCC. Red team to always have an APRS tracker.

0843h to 0848h X Day	**(Blue Team)** – Cdr and staff to undertake detection of Red Team through available video feed at TCC – interdict decision by Cdr when Red Team crosses IB.	

Time	Event Description and Action	Remarks
0849h X Day	**Control Team** – to Cdr – Infiltration of Harruki militants from sector ZULU confirmed. **Control Team** – Red Team to commence movement from GR _____ to BCP1. Use available local camouflage during move.	
0850h X Day	**Cdr** – Sensor Boss – Give latest update now – confirm detection of Harruki movement by MicroObserver sensors. Provide video feed from ground sensor to TCC immediately on detection of Harruki. **Cdr** – Air Boss – Redirect bird to cover area from BCP1 to West up to IB – confirm detection of Harruki. **Cdr** – Balloon Boss – Tilt cameras towards BCP1	
0851h to 0855h X Day	**(Blue Team)** – Cdr and staff to undertake detection of Red Team through available video feed at TCC – interdict decision by Cdr to be given to Ground and Post Boss on confirmed detection.	
0856h X Day	**Control Team** – to Cdr – Unidentified persons seen approaching BCP1 from the West – ensure identification checks carried out at BCP1.	
0857h X Day	**Cdr** – Post Boss – Carry out identification checks of all unidentified persons and pass report to TCC immediately.	
0858h X Day	**Post Boss** – Five unidentified persons apprehended at BCP1, forensics identification being undertaken.	
0859h X Day	**Post Boss** – Video feed now available at TCC – fingerprint and visual identification data forwarded to TCC – awaiting confirmation.	
0900h to 0903h X Day	**(Blue Team)** – Cdr and staff to undertake confirmation of forensic data and confirm match.	
Scenario – Part II – Operations in Area TANGO		
0905h X Day	**Control Team** – to Cdr – Red Team consisting of five members successful in infiltrating through area TANGO and has been seen in Hara village carrying a wooden box. The team members are wearing civilian clothes and are likely to move south towards Chiang Mai using vehicular transport. The local police has apprehended two suspects without the necessary identification documents – a Biometric Team maybe required to confirm identification of suspected persons.	Actual roads and tracks used by Red Team will be indicated on ground in consultation with Thai officials.
0907h X Day	**Cdr** – Air Boss – UAV surveillance required over area TANGO immediately – await further orders. **Cdr** – Post Boss – Move one Forensic Team to Hara village, Team to merry up with village headman and local police and carryout identification of apprehended personnel. **Cdr** – Ground Boss – Move troops to conduct a Cordon and Search Operation at Hara village – five suspected Harraki militants likely to be present. **Air Boss** – UAV Boss - Execute launch bird immediately and proceed to TANGO sector and loiter on station until further notice. Ensure video surveillance commences when bird is on station. Also, redirect bird from ZULU sector to loiter over TANGO sector.	
0908h X Day	**UAV Boss** – Bird launched for TANGO sector and another redirected from ZULU sector. Video feed will be available once birds are on station.	

Post Boss – One Forensic Team detached from BCP2 and is moving to Hara village. Forensic data will be forwarded as soon as Team reaches location.
Ground Boss – I am on my way to Hara village with a platoon – cordon likely to be established by 0940h – cordon party equipped with hand held terminals – shall report once cordon is established and search is commenced.

Time	Event Description and Action	Remarks
0909h to 0915h X day	**Forensic Team** – Reached location – suspects being tested – await forensic data. **Ground Boss** – Cordon established – stops in location – search party commencing operation.	
0916h X Day	**Control** – Harraki militants spotted in Hara village and are moving South in a White truck using available unpaved roads .	
0917h X Day	**Cdr** – Air Boss – Instruct birds to cover tracks leading south from Hara village – Harraki militants using White truck.	
0918h X Day	**Air Boss** - UAV Boss – Birds to cover roads and tracks leading south from Hara village – target is a white truck. **UAV Boss** – Birds covering tracks now – video feed now available.	
0919h to 0930h X Day	**(Blue Team)** – Cdr and staff to undertake detection of vehicle used by Harraki militants through available video feed at TCC – interdict decision by Cdr to be given to Ground Boss on confirmed detection.	
Scenario – Part III – Operations in Area ECHO		
0935h X Day	**Control Team** – to Cdr – The district administration in the Mae Ngat area has approached the Blue Land Forces to undertake an aerial reconnaissance of the flood ravaged area in ECHO sector in order to look for people trapped in the river.	
0935h X Day	**Cdr** – to Air Boss – UAV reconnaissance mission required in Area ECHO – search for people trapped on boats, wooden logs, etc due to the floods in the area. Deploy assets immediately to cover the entire area.	
0936h X Day	**Air Boss** – to UAV Boss – get Cyberbug and other UAV assets over Area ECHO – mission is to find flood survivors.	
0937h to 0950h X day	(UAVs launched in Area ECHO – Cdr and staff undertake detection of survivors in the area)	Two boats required in Area ECHO to depict survivors.

LIST OF REFERENCES

Alberts, Garstka and Stein, "Network Centric Warfare: Developing and Leveraging information Superiority." CCRP. February 2000.

Bradford, Bryan L. "Wireless Security within Hastily Formed Networks." Naval Postgraduate School, Monterey, CA. September 2006.

Caceres, Francisco, and Swearingen, Brad "Analysis of the 802.11b and IEEE 802.16 Technologies as a part of the Tactical Internet." Naval Postgraduate School (NPS). Monterey, CA. September 2005.

Chief of Naval Operations (CNO), "Guidance for 2007: Focus on Execution." February 2, 2007.

Clark, Vern ADM. "Projecting Decisive Joint Capabilities – Sea Power 21 Series Part I." Proceedings. Naval Institute. Annapolis, MD. October 2002.

"COASTS Concept of Operations 2007." Naval Postgraduate School. Monterey, CA. April 24, 2007.

"COASTS-07 Executive White Paper." Naval Postgraduate School. Monterey, CA. November 18, 2006.

"COASTS After Action Report." Naval Postgraduate School. Monterey, CA. July 4, 2006.

Comer, Douglas E. Computer Networks and Internets with Internet Applications. Pearson Education Inc. Upper Saddle River, NJ. 2004.

Department of Defense C4ISR Architecture Working Group (AWG) Version 2. December 18, 1997.

Department of Homeland Security. "U.S. Coast Guard Biometrics at Sea." November 3, 2006.

Guice, Robert J., and Munoz, Ramon J. "IEEE 802.16 Commercial off the Shelf (COTS) Technologies as a Complement to Objective Maneuver (STOM) Communications." Naval Postgraduate School, Monterey, CA. September 2004.

Hochstedler, Robert "Implementation of a Modular Fly Away Kits (FLAK) for C4ISR in Order to Counter Asymmetric Threats in the Coalition Riverine and Maritime Theatres." Naval Postgraduate School, Monterey, CA. June 2006.

IEEE Standard for Conformance to IEEE 802.16, *Part 1: Protocol Implementation Conformance Statement (PICS) Proforma for 10-66 GHz WirelessMAN-SC Air Interface.* August 18, 2003.

"The Implementation of Network-Centric Warfare." Director, Force Transformation, Office of the Secretary of Defense. Department of Defense. Washington, DC. January 5, 2005.

Kelley, Sean W. "An Analysis of the use of Medical Applications Required for Complex Humanitarian Disasters or Emergencies via hastily Formed Networks (HFN) in the Field." Naval Postgraduate School, Monterey, CA. September 2005.

"Joint Vision: 2020." Joint Chiefs of Staff (JCS). Department of Defense (DoD). Washington, DC. June 2000.

Klopson, Jadon E. and Burdian, Stephen V. "Collaborative Applications used in a Wireless Environment at Sea for use in Coast Guard Law Enforcement and Homeland Security Missions." Naval Postgraduate School, Monterey, CA. March 2005.

Lancaster, David D. "Developing a Fly-Away Kit (FLAK) to Support Hastily Formed Networks (HFN) for Humanitarian Assistance and Disaster Relief (HA/DR). Naval Postgraduate School, Monterey, CA. June 2006.

"National Security Strategy (2006)." Washington, D.C. March 2006.

"National Strategy for Homeland Security. Washington, D.C. July 2002.

"The National Strategy for Maritime Security." United States Coast Guard (USCG). Washington D.C. September 2005.

Naval Ships' Technical Manual. "Boats and Small Craft." Chapter 583, Volume 1, Revision 5. December 2001.

Parachini, John V., Davis, Lynn E., Liston, Timothy. "Homeland Security: A Compendium of Public and Private Organizations' Policy Recommendations." RAND. Pittsburgh, PA. 2003.

"Quadrennial Defense Review Report." Washington, D.C. February 6, 2006.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Mr. James F. Ehlert
   Director, Maritime Domain Protection Research Group (MDP-RG)
   Naval Postgraduate School
   Monterey, California,

4. Colonel Thomas Lee Williams
   Deputy Science Advisor
   U.S. Pacific Command (USPACOM)
   Camp Smith, Hawaii

5. RADM Paul F. Zukunft
   Director
   Joint Inter-Agency Task Force West (JIATF-W)
   Camp Smith, Hawaii

6. Mr. Kurt Badescher
   US Special Operations Command (USSOCOM)
   Tampa, Florida

7. Mr. J. Christopher Griffin,
   Westwood Computer Corporation
   Charlotte, North Carolina

8. Mr. Ralph L. Boyce, US Ambassador of Thailand
   US Department of State (DoS)
   Bangkok Thailand

9. Lt Col Mel Prell, USAF
   Office of Defense Cooperation
   Jakarta, Indonesia

10. Lieutenant General Apichart
    Director-General, Defence Research & Development Office (DRDO)
    Parkred, Nonthaburi

11. Group Captain Dr. Triroj Virojtriratana
DRDO COASTS Project Manager
Parkred, Nonthaburi,

12. Group Captain Wanchai Tosuwan
Director, Research & Development Promotion Division
Parkred, Nonthaburi,

13. Group Captain Teerachat Krajomkeaw
Directorate of Operations
Royal Thailand Air Force (RTAF) Headquarters
Bangkok, Thailand

14. Mr. Robert Sandoval
Joint Intelligence Operations Command (JIOC)
San Antonio, Texas

15. John Taylor
President, Mercury Data Systems
Greensboro, North Carolina

16. Major Phil Erdie, USMC
U.S. Marine Corp Systems Command (MARCORSYSCOM)
Quantico, Virginia

17. Mr. Thomas Latta
C4ISR & IO PM
Space and Naval Warfare Systems Command
Norfolk, Virginia

18. RADM Nimmick, USCG
Maritime Intelligence Fusion Center (MIFC)
Alameda, California

19. Mr. Curtis White
Commander's Representative
USAF Force Protection Battle Lab
Lackland AFB, Texas

20. USCG Headquarters
Washington, DC
Att: MCPO Wright

21. Mr. Andre Obradovic
Senior Manager, Defence Initiatives ASIA Pacific
Cisco Systems

22. Mr. Mike Rathwell
Identix Corporation
Jersey City, New Jersey

23. Dr. Leonard Ferrari
Provost
Naval Postgraduate School
Monterey, California

24. Dr. Pat Sankar
NPS Distinguished Fellow
Naval Postgraduate School
Monterey, California

25. Dr. Gurminder Singh
Director of the Center for the Study of Mobile Devices and Communications
Naval Postgraduate School
Monterey, California

26. Dr. Frank Shoup
Director of Research, Meyers Institute, GSEAS
Naval Postgraduate School
Monterey, California

27. Dr. Dan Boger
Chairman of the Graduate School of Information Sciences
Naval Postgraduate School
Monterey, California

28. Pat Gleeson
EDS - Navy Marine Corps Intranet (NMCI)
USMC Operations Analyst
New Orleans, Louisiana

29. Mr. Phillip Ardire
President, Western DataCom
Westlake, Ohio